HP ProtectTools

Einführung

Erste Ausgabe: Januar 2011

Teilenummer des Dokuments: 638391-041

Inhaltsverzeichnis

1 Einführung in die Sicherheitsfunktionen

Die HP ProtectTools Security Manager Software bietet Sicherheitsfunktionen, die den Computer, Netzwerke und wichtige Daten vor unberechtigtem Zugriff schützen.

Anwendung	Funktionen
HP Protect Tools Administrator-Konsole (für Administratoren)	• Administratorrechte unter Microsoft Windows sind für den Zugriff erforderlich. • Bietet Zugriff auf Module, die von einem Administrator konfiguriert werden und für Benutzer nicht verfügbar sind. • Ermöglicht eine erste Sicherheitseinrichtung und die Konfiguration von Optionen oder Anforderungen für alle Benutzer.
HP ProtectTools Security Manager (für Benutzer)	• Ermöglicht einem Benutzer, Optionen zu konfigurieren, die von einem Administrator bereitgestellt wurden. • Ermöglicht Administratoren, Benutzern die eingeschränkte Steuerung einiger HP ProtectTools Softwaremodule zu ermöglichen.

Welche Softwaremodule für Ihren Computer verfügbar sind, ist vom Modell abhängig.

Die HP ProtectTools Softwaremodule sind möglicherweise vorinstalliert oder bereits geladen, oder sie sind auf der HP Website zum Download verfügbar. Weitere Informationen finden Sie unter http://www.hp.com.

HINWEIS: Bei den Anleitungen in diesem Handbuch wird davon ausgegangen, dass die HP ProtectTools Softwaremodule bereits installiert sind.

HP ProtectTools Funktionen

In der folgenden Tabelle finden Sie nähere Informationen zu den HP ProtectTools Modulen.

Modul	Funktionen
HP ProtectTools Administrator-Konsole (für Administratoren)	• Sicherheitsebenen und Sicherheits-Anmeldemethoden mithilfe des Installations-Assistenten von Security Manager einrichten und konfigurieren. • Optionen, die für Benutzer nicht sichtbar sind, konfigurieren. • Device Access Manager Konfigurationen und Benutzerzugriffseinstellungen einrichten. • HP ProtectTools Benutzer hinzufügen und entfernen und Benutzerstatus mithilfe der Funktion Administrator-Tools anzeigen.
HP ProtectTools Security Manager (für Benutzer)	• Kennwörter verwalten, einrichten und ändern. • Benutzerberechtigungen, wie Windows Kennwort, Fingerabdruck oder Smart Card, konfigurieren und ändern. • Optionen zum Shreddern und Überschreiben in File Sanitizer und andere Einstellungen konfigurieren und ändern. • Einstellungen für Device Access Manager anzeigen. • Computrace for HP ProtectTools konfigurieren. • Voreinstellungen und Sicherungs- sowie Wiederherstellungsoptionen konfigurieren.
Credential Manager for HP ProtectTools (Password Manager)	• Benutzernamen und Kennwörter sichern, verwalten und schützen. • Anmeldebildschirme von Websites und Programmen für den schnellen und sicheren Zugriff einrichten. • Website-Benutzernamen und -Kennwörter speichern, indem sie in Password Manager eingegeben werden. Wenn Sie diese Website das nächste Mal besuchen, gibt Password Manager die Daten automatisch ein und übermittelt sie. • Stärkere Kennwörter für eine höhere Kontosicherheit erstellen. Password Manager füllt die Informationen automatisch aus und übermittelt sie.
Drive Encryption for HP ProtectTools (bestimmte Modelle)	• Bietet eine komplette Verschlüsselung der gesamten Festplatte. • Erzwingt eine Authentifizierung vor dem Systemstart zum Entschlüsseln und Zugreifen auf Daten.
File Sanitizer for HP ProtectTools	• Shreddert digitale Bestände (sensible Informationen wie Anwendungsdateien, historischen oder Web-bezogenen Inhalt und andere vertrauliche Daten) auf Ihrem Computer und überschreibt von Zeit zu Zeit Datenbestände auf der Festplatte.

Modul	Funktionen
Device Access Manager for HP ProtectTools (nur ausgewählte Modelle)	• Ermöglicht IT-Managern die Zugriffssteuerung von Geräten auf Basis von Benutzerprofilen. • Verhindert, dass Daten von nicht autorisierten Benutzern auf externe Speichermedien kopiert werden und Viren über externe Medien in das System gelangen. • Ermöglicht Administratoren, den Zugriff auf beschreibbare Geräte für bestimmte Personen oder Benutzergruppen zu sperren.
Privacy Manager for HP ProtectTools (bestimmte Modelle)	• Generiert Echtheitszertifikate, mit denen die Quelle, Integrität und Sicherheit der Verbindung überprüft wird, wenn Microsoft E-Mail und Microsoft Office-Dokumente verwendet werden.
Computrace for HP ProtectTools (separat erhältlich)	• Bietet sichere Bestandsverfolgung. • Überwacht Benutzeraktivität sowie Hardware- und Softwareänderungen. • Bleibt aktiv, auch wenn die Festplatte neu formatiert oder ersetzt wird. • Für die Aktivierung ist ein separates Tracking- and Tracing-Abonnement erforderlich.
Embedded Security for HP ProtectTools (nur ausgewählte Modelle)	• Verwendet einen integrierten TPM-Sicherheitsschip (Trusted Platform Module) zum Schutz gegen den nicht autorisierten Zugriff auf Benutzerdaten und Anmeldeinformationen, die auf einem Computer gespeichert sind. • Ermöglicht die Erstellung eines persönlichen sicheren Laufwerks (PSD, Personal Secure Drive), mit dem sich Informationen in Benutzerdateien und -ordnern wirksam schützen lassen. • Unterstützt Anwendungen von Drittanbietern (wie Microsoft Outlook und Internet Explorer) für geschützte Vorgänge, bei denen digitale Zertifikate zum Einsatz kommen.

HP ProtectTools – Beschreibung und allgemeine Nutzungsbeispiele der Sicherheitsprodukte

Die meisten der HP ProtectTools Sicherheitsprodukte verfügen sowohl über die Benutzerauthentifizierung (normalerweise ein Kennwort) als auch über ein Administrator-Backup, um den Zugriff zu gewährleisten, wenn Kennwörter verloren gehen, nicht verfügbar sind oder vergessen wurden, oder wenn die Unternehmenssicherheit einen Zugriff erforderlich macht.

HINWEIS: Einige der HP ProtectTools Sicherheitsprodukte dienen der Zugriffsbeschränkung auf Daten. Daten sollten verschlüsselt werden, wenn sie so wichtig sind, dass der Benutzer sie lieber verlieren würde, als sie an andere weiterzugeben. Es wird empfohlen, ein Backup aller Daten an einem sicheren Ort aufzubewahren.

Credential Manager for HP ProtectTools

Credential Manager (Teil von Security Manager) speichert Benutzernamen und Kennwörter und lässt sich für Folgendes einsetzen:

- Speichern von Anmeldenamen und Kennwörtern für den Internetzugriff und E-Mails.
- Automatische Anmeldung des Benutzers bei einer Website oder E-Mail.
- Verwalten und Organisieren von Authentifizierungen.
- Auswahl eines Web- oder Netzwerkbestands und direkter Zugriff auf den Link.
- Anzeigen von Namen und Kennwörtern, wenn erforderlich.

Beispiel 1: Die Einkaufssachbearbeiterin eines großen Herstellers tätigt die meisten ihrer Unternehmenstransaktionen über das Internet. Sie besucht auch häufig verschiedene Websites, für die Anmeldeinformationen erforderlich sind. Sie achtet genau auf Sicherheit, benutzt also nicht für jedes Konto das gleiche Kennwort. Die Einkaufssachbearbeiterin hat sich entschieden, Credential Manager zu verwenden, um Weblinks mit verschiedenen Benutzernamen und Kennwörtern abzugleichen. Wenn sie sich auf einer Website anmeldet, übermittelt Credential Manager automatisch die Zugriffsdaten. Wenn sie den Benutzernamen und das Kennwort abrufen möchte, kann Credential Manager dazu konfiguriert werden, sie anzuzeigen.

Credential Manager kann auch zum Verwalten und Organisieren der Authentifizierungen verwendet werden. Das Tool ermöglicht einem Benutzer die Auswahl eines Web- oder Netzwerkbestands und den direkten Zugriff auf den Link. Der Benutzer kann gegebenenfalls Namen und Kennwörter abrufen.

Beispiel 2: Ein Buchprüfer wurde befördert und leitet nun die gesamte Buchhaltung. Das Team muss sich bei einer Vielzahl an Client-Webkonten anmelden, für die verschiedene Anmeldeinformationen erforderlich sind. Diese Anmeldeinformationen werden mit anderen Angestellten gemeinsam genutzt, Vertraulichkeit ist also ein Thema. Der Buchhalter entscheidet sich, alle Weblinks, Benutzernamen im Unternehmen und Kennwörter mit Credential Manager for HP ProtectTools zu verwalten. Sobald er damit fertig ist, verteilt der Buchhalter Credential Manager an die Angestellten, damit sie mit den Webkonten arbeiten können, die von ihnen verwendeten Anmeldedaten aber nicht kennen.

Drive Encryption for HP ProtectTools

Drive Encryption dient zur Zugriffseinschränkung auf die Daten der gesamten Computerfestplatte oder eines Zweitlaufwerks. Drive Encryption kann auch selbstverschlüsselnde Laufwerke verwalten.

Beispiel 1: Ein Arzt möchte sicherstellen, dass nur er Zugriff auf die Daten auf seiner Computerfestplatte hat. Er aktiviert Drive Encryption, was eine Authentifizierung vor dem Systemstart noch vor der Anmeldung bei Windows erforderlich macht. Nach der Einrichtung ist kein Zugriff auf die Festplatte ohne Angabe eines Kennworts vor dem Start des Betriebssystems mehr möglich. Der Arzt kann die Laufwerkssicherheit noch weiter verbessern, wenn er die Daten mit der SED-Option (selbstverschlüsselndes Laufwerk) verschlüsselt.

Sowohl Embedded Security for HP ProtectTools als auch Drive Encryption for HP ProtectTools sperren den Zugriff auf die verschlüsselten Daten, auch wenn das Laufwerk entfernt wird, weil beide an die Original-Hauptplatine gebunden sind.

Beispiel 2: Der Verwaltungschef eines Krankenhauses möchte sicherstellen, dass nur Ärzte und autorisierte Mitarbeiter auf die Daten auf ihrem lokalen Computer zugreifen können, ohne ihre persönlichen Kennwörter anderen preisgeben zu müssen. Die IT-Abteilung fügt den Administrator, die Ärzte und alle autorisierten Mitarbeiter als Drive Encryption-Benutzer hinzu. Jetzt können nur noch autorisierte Mitarbeiter den Computer oder die Domäne mit ihrem persönlichen Benutzernamen und Kennwort starten.

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools wird verwendet, um Daten permanent zu löschen, einschließlich Internet-Browseraktivität, temporären Dateien, bereits gelöschten Dateien und anderen Informationen. File Sanitizer kann so konfiguriert werden, dass er entweder manuell oder automatisch nach einem benutzerdefinierten Zeitplan läuft.

Beispiel 1: Ein Anwalt hat oft mit sensiblen Klienteninformationen zu tun und möchte sicherstellen, dass gelöschte Dateien nicht wiederhergestellt werden können. Er verwendet File Sanitizer, um gelöschte Dateien zu „shreddern“, so dass es nahezu unmöglich ist, sie wiederherzustellen.

Wenn Daten unter Windows gelöscht werden, werden sie normalerweise nicht von der Festplatte entfernt. Stattdessen werden die entsprechenden Sektoren der Festplatte für die zukünftige Verwendung als verfügbar gekennzeichnet. Bis die Daten überschrieben werden, können sie mit Tools, die im Internet verfügbar sind, wiederhergestellt werden. File Sanitizer überschreibt die Sektoren mit Zufallsdaten (mehrmals, wenn nötig) und macht sie so unlesbar und nicht wiederherstellbar.

Beispiel 2: Eine Forscherin möchte gelöschte Daten, temporäre Dateien, Browseraktivität usw. automatisch löschen, sobald sie sich abmeldet. Sie verwendet File Sanitizer, um das Shreddern zeitlich zu planen, und kann so allgemeine Dateien oder bestimmte Dateien auswählen, die automatisch gelöscht werden sollen.

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools kann dazu verwendet werden, den nicht autorisierten Zugriff auf USB-Flash-Laufwerke zu verhindern, wenn Daten kopiert werden könnten. Er kann auch den Zugriff auf CD/DVD-Laufwerke und die Steuerung von USB-Geräten, Netzwerkverbindungen usw. einschränken. Ein Administrator kann festlegen, wann oder wie lange Laufwerke zugänglich sind. Ein Beispiel wäre eine Situation, in der andere Hersteller Zugriff auf einen Unternehmenscomputer benötigen, aber nicht in der Lage sein sollen, Daten auf ein USB-Laufwerk zu kopieren. Device Access Manager for HP ProtectTools ermöglicht es einem Administrator, den Zugriff auf die Hardware einzuschränken und zu verwalten.

Beispiel 1: Der Manager eines Unternehmens für medizinischen Bedarf arbeitet neben seinen Unternehmensdaten auch oft mit Krankenakten. Die Angestellten benötigen Zugriff auf diese Daten, es ist aber extrem wichtig, dass die Daten nicht mit einem USB-Laufwerk oder einem anderen externen Speichermedium vom Computer entfernt werden können. Das Netzwerk ist sicher, aber die

Computer haben CD-Brenner und USB-Anschlüsse, die es ermöglichen, die Daten zu stehlen oder zu kopieren. Der Manager verwendet Device Access Manager, um die USB-Anschlüsse und CD-Brenner zu deaktivieren, damit sie nicht benutzt werden können. Obwohl die USB-Anschlüsse gesperrt sind, bleiben Maus und Tastatur funktionsfähig.

Beispiel 2: Ein Versicherungsunternehmen möchte verhindern, dass die Angestellten persönliche Software oder Daten von Zuhause installieren oder laden. Einige Angestellte benötigen auf allen Computern Zugriff auf den USB-Anschluss. Der IT-Manager verwendet Device Access Manager, um den Zugriff für einige Angestellte zu ermöglichen und gleichzeitig den externen Zugriff für andere zu sperren.

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools wird verwendet, wenn die E-Mail-Kommunikation über Internet gesichert werden muss. Der Benutzer kann E-Mails erstellen und senden, die sich nur von einem authentifizierten Empfänger öffnen lassen. Privacy Manager verhindert, dass die Informationen durch einen Betrüger abgefangen oder gefährdet werden.

Beispiel 1: Ein Börsenmakler möchte sicherstellen, dass seine E-Mails nur an bestimmte Kunden gesendet werden und dass niemand das E-Mail-Konto manipulieren oder Informationen abfangen kann. Der Börsenmakler meldet sich und seine Kunden bei Privacy Manager an. Privacy Manager stellt jedem Benutzer ein Authentifizierungszertifikat (CA) aus. Mit diesem Tool müssen der Börsenmakler und seine Kunden sich authentifizieren, bevor E-Mails ausgetauscht werden können.

Mit Prrivacy Manager for HP ProtectTools können E-Mails auf einfache Weise gesendet und empfangen werden, wenn der Empfänger verifiziert und authentifiziert wurde. Der Mailservice lässt sich auch verschlüsseln. Die Verschlüsselung verläuft ähnlich wie bei Kreditkartenkäufen über das Internet.

Beispiel 2: Ein Vorstandschef möchte sicherstellen, dass nur die Mitglieder des Vorstands Informationen anzeigen können, die er per E-Mail versendet. Er verwendet die Option zur Verschlüsselung von E-Mails, die von den Vorstandsmitgliedern empfangen und an ihn gesendet werden. Ein Privacy Manager Authentifizierungszertifikat ermöglicht es allen Vorstandsmitglieder, eine Kopie des Verschlüsselungsschlüssels zu besitzen, damit nur sie die vertraulichen E-Mails entschlüsseln können.

Computrace for HP ProtectTools (zuvor LoJack Pro)

Computrace for HP ProtectTools ist ein Service (separat erhältlich), der die Position eines gestohlenen Computers bestimmen kann, sobald der Benutzer auf das Internet zugreift.

Beispiel 1: Ein Schuldirektor hat die IT-Abteilung damit beauftragt, alle Computer an seiner Schule zu verfolgen. Nach der Bestandsaufnahme der Computer hat der IT-Administrator alle Computer bei Computrace registriert, so dass sie sich im Fall eines Diebstahls verfolgen lassen. Kürzlich stellte die Schule fest, dass mehrere Computer fehlen. Der IT-Administrator setzte also die Behörden und Computrace-Mitarbeiter davon in Kenntnis. Die Computer wurden gefunden und von den Behörden der Schule zurückgebracht.

Computrace for HP ProtectTools dient auch dazu, Computer per Fernzugriff zu verwalten und aufzufinden sowie die Nutzung von Computern und Anwendungen zu überwachen.

Beispiel 2: Eine Immobiliengesellschaft muss weltweit Computer verwalten und aktualisieren. Sie verwendet Computrace, um die Computer zu überwachen und zu aktualisieren, ohne dazu einen IT-Mitarbeiter zu jedem Computer schicken zu müssen.

Embedded Security for HP ProtectTools (nur ausgewählte Modelle)

Embedded Security for HP ProtectTools bietet die Möglichkeit, ein persönliches sicheres Laufwerk anzulegen. Diese Funktion ermöglicht es dem Benutzer, eine virtuelle Laufwerkspartition auf dem PC einzurichten, die bis zum Zugriff komplett verborgen bleibt. Embedded Security kann überall verwendet werden, wo ein Teil der Daten geheim geschützt werden muss, ohne den Rest der Daten zu verschlüsseln.

Beispiel 1: Der Manager eines Lagerhauses hat einen Computer, auf welchen den ganzen Tag lang verschiedene Angestellte zugreifen. Der Manager möchte vertrauliche Daten des Lagerhauses auf dem Computer verschlüsseln und ausblenden. Er möchte, dass die Daten so sicher sind, dass sie auch bei einem Diebstahl der Festplatte nicht entschlüsselt und gelesen werden können. Er beschließt, Embedded Security zu aktivieren, und verschiebt die vertraulichen Daten auf das persönliche sichere Laufwerk. Der Manager kann ein Kennwort eingeben und auf die vertraulichen Daten wie auf jedes andere Laufwerk zugreifen. Wenn er sich abmeldet oder das persönliche sichere Laufwerk neu startet, können die Daten ohne Angabe des Kennworts nicht abgerufen werden. Die Angestellten bekommen die vertraulichen Daten nie zu Gesicht, wenn sie auf den Computer zugreifen.

Embedded Security schützt Verschlüsselungsschlüssel innerhalb eines TPM-Chips (Trusted Platform Module), der sich auf der Hauptplatine befindet. Es ist das einzige Verschlüsselungstool, das den Mindestanforderungen genügt, um Kennwortattacken zu widerstehen, wenn jemand versucht, das Verschlüsselungskennwort zu erraten. Embedded Security kann auch die gesamte Festplatte und E-Mails verschlüsseln.

Beispiel 2: Eine Börsenmaklerin möchte extrem sensible Daten mit einem portablen Laufwerk auf einen anderen Computer übertragen. Sie möchte sicherstellen, dass nur diese beiden Computer das Laufwerk öffnen können, selbst wenn das Kennwort bekannt wird. Sie verwendet die TPM-Migration von Embedded Security, um einem zweiten Computer zu ermöglichen, die Verschlüsselungsschlüssel zum Entschlüsseln der Daten zu besitzen. Während der Übertragung können auch mit Kennwort nur diese beiden physischen Computer die Daten entschlüsseln.

Lösungen für grundlegende Sicherheitsaufgaben

Die HP ProtectTools Module bieten zusammengenommen Lösungen für eine Vielzahl von Sicherheitsproblemen. Hierzu zählen auch die folgenden grundlegenden Sicherheitsmaßnahmen:

- Schutz gegen Diebstahl
- Einschränken des Zugriffs auf sensible Daten
- Verhindern des unbefugten Zugriffs von internen oder externen Standorten
- Erstellen von Richtlinien für den starken Kennwortschutz

Schutz vor gezieltem Diebstahl

Ein Beispiel für gezielten Diebstahl ist der Diebstahl eines Computers mit vertraulichen Daten und Kundeninformationen an einer Sicherheitskontrolle eines Flughafens. Die folgenden Merkmale helfen Ihnen, Ihren Computer vor gezieltem Diebstahl zu schützen:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem. Siehe die folgenden Kapitel:
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Die Funktion des persönlichen sicheren Laufwerks, die vom Modul Embedded Security for HP ProtectTools bereitgestellt wird, verschlüsselt sensible Daten, um sicherzustellen, dass niemand ohne Authentifizierung darauf zugreifen kann. Nähere Informationen dazu erhalten Sie im Kapitel:
  - Embedded Security for HP ProtectTools
- Computrace kann die Position eines Computers nach einem Diebstahl feststellen. Nähere Informationen dazu erhalten Sie im Kapitel:
  - Computrace for HP ProtectTools

Einschränken des Zugriffs auf sensible Daten

Nehmen wir an, ein Vertragsprüfer arbeitet vor Ort und hat Zugriff auf den Computer zur Überprüfung sensibler Finanzdaten erhalten. Er soll ihm aber nicht möglich sein, die Dateien zu drucken oder auf eine CD zu kopieren. Die folgende Funktion schränkt den Zugriff auf die Daten ein:

- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf Schreibgeräte einzuschränken, so dass sensible Daten nicht gedruckt oder von der Festplatte auf ein Wechselmedium kopiert werden können.

Verhindern des unbefugten Zugriffs von internen oder externen Standorten

Der unautorisierte Zugriff auf einen nicht gesicherten Unternehmenscomputer stellt ein großes Risiko für die Ressourcen im Unternehmensnetzwerk dar, wie beispielsweise für die Daten von Finanzdienstleistern, einer Behörde oder der Abteilung für Forschung & Entwicklung, sowie für

vertrauliche Informationen wie Patientendatensätze oder persönliche Finanzdaten. Die folgende Funktion verhindert den unautorisierten Zugriff:

- Die Funktion zur Authentifizierung vor dem Systemstart verhindert den Zugriff auf das Betriebssystem. Siehe die folgenden Kapitel:
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Mit Password Manager können Sie sicherstellen, dass unberechtigte Benutzer keine Kennwörter bzw. keinen Zugriff auf kennwortgeschützte Anwendungen erhalten.
- Device Access Manager for HP ProtectTools ermöglicht es IT-Managern, den Zugriff auf Schreibgeräte einzuschränken, so dass sensible Daten nicht von der Festplatte kopiert werden können.
- File Sanitizer ermöglicht das sichere Löschen von Daten durch Shreddern kritischer Dateien und Ordner bzw. Überschreiben von gelöschten Beständen auf der Festplatte (Daten, die gelöscht wurden, aber wiederherstellbar sind, werden überschrieben).
- Privacy Manager ist ein Tool zur Erstellung von Echtheitszertifikaten, wenn Sie Microsoft E-Mail oder Microsoft Office-Dokumente verwendet werden, damit wichtige Informationen sicher gesendet und gespeichert werden.

Erstellen von Richtlinien für starke Kennwörter

Wenn eine Unternehmensrichtlinie in Kraft tritt, die das Benutzen starker Kennwörter für Web-basierte Anwendungen und Datenbanken erforderlich macht, bietet Security Manager ein geschütztes Repository für Kennwörter und Single Sign-On.

Weitere Sicherheitselemente

Zuweisen von Sicherheitsrollen

Bei der Verwaltung der Computersicherheit (besonders für große Unternehmen) besteht ein wichtiger Faktor darin, die Zuständigkeiten und Berechtigungen auf verschiedene Typen von Administratoren und Benutzern zu verteilen.

HINWEIS: In kleineren Unternehmen oder im heimischen Büro können diese Rollen selbstverständlich auch alle von einer Person wahrgenommen werden.

Bei HP ProtectTools können die Pflichten und Berechtigungen in folgende Rollen unterteilt werden:

- Der Sicherheitsbeauftragte definiert die Sicherheitsstufe für das Unternehmen oder Netzwerk und bestimmt die Sicherheitsfunktionen, die bereitgestellt werden sollen, wie Drive Encryption oder Embedded Security.

  HINWEIS: Viele Funktionen in HP ProtectTools können vom Sicherheitsbeauftragten in Zusammenarbeit mit HP noch weiter angepasst werden. Weitere Informationen finden Sie auf der HP Website unter http://www.hp.com.

- Der IT-Administrator wendet die vom Sicherheitsbeauftragten definierten Sicherheitsfunktionen an und verwaltet sie. Er kann auch einige Funktionen aktivieren oder deaktivieren. Wenn der Sicherheitsbeauftragte zum Beispiel entschieden hat, Smart Cards bereitzustellen, kann der IT-Administrator das Kennwort und den Smart Card-Modus aktivieren.
- Der Benutzer nutzt die Sicherheitsfunktionen. Wenn der Sicherheitsbeauftragte und der IT-Administrator zum Beispiel Smart Cards für das System aktiviert haben, kann der Benutzer die PIN für die Smart Card festlegen und die Karte zur Authentifizierung benutzen.

ACHTUNG: Administratoren wird geraten, gemäß den „Best Practices“ die Rechte für Endbenutzer und den Benutzerzugriff einzuschränken.

Unberechtigte Benutzer sollten nicht über Administratorrechte verfügen.

Verwalten der Kennwörter für HP ProtectTools

Die meisten HP ProtectTools Security Manager Funktionen sind durch Kennwörter geschützt. Die folgende Tabelle enthält die gängigsten Kennwörter, die Softwaremodule, für welche die Kennwörter eingerichtet wurden, sowie die Kennwortfunktion.

Die Kennwörter, die nur vom IT-Administrator eingerichtet und verwendet werden können, werden ebenfalls in dieser Tabelle angegeben. Alle anderen Kennwörter können von normalen Benutzern oder Administratoren eingerichtet werden.

HP ProtectTools Kennwort	Wird in diesem Modul eingerichtet	Funktion
Windows Anmeldekennwort	Windows® Systemsteuerung oder HP ProtectTools Security Manager	Zur manuellen Anmeldung oder zur Authentifizierung, um auf verschiedene Security Manager Funktionen zuzugreifen.
Sicherungs- und Wiederherstellungskennwort für Security Manager	Security Manager, vom Benutzer selbst	Schützt den Zugriff auf die Security Manager Sicherungs- und Wiederherstellungsdatei.

HP ProtectTools Kennwort	Wird in diesem Modul eingerichtet	Funktion
Smart Card-PIN	Credential Manager	Kann zur Mehrfach-Authentifizierung verwendet werden. Kann zur Windows Authentifizierung verwendet werden. Authentifiziert Benutzer von Drive Encryption, wenn das Smart Card-Token ausgewählt wird.
Kennwort für Notfallwiederherstellungs-Token	Embedded Security, durch IT-Administrator	Schützt den Zugriff auf das Notfallwiederherstellungs-Token, eine Sicherungsdatei für den integrierten Sicherheitschip.
Kennwort des Eigentümers	Embedded Security, durch IT-Administrator	Schützt das System und den TPM-Chip vor nicht autorisiertem Zugriff auf alle Eigentümerfunktionen von Embedded Security.
BIOS-Administrator-Kennwort	Computer Setup, durch IT-Administrator	Schützt den Zugriff auf Computer Setup Utility.

Erstellen eines sicheren Kennworts

Das Einrichten von Kennwörtern ist nur möglich, wenn Sie die vom Programm festgelegten Anforderungen erfüllen. Beachten Sie im Allgemeinen folgende Richtlinien für das Einrichten von sicheren Kennwörtern, um die Risiken in Bezug auf Kennwörter zu verringern:

- Verwenden Sie Kennwörter mit mehr als 6 Zeichen, vorzugsweise mehr als 8 Zeichen.
- Mischen Sie im gesamten Kennwort Klein- und Großbuchstaben.
- Verwenden Sie nach Möglichkeit sowohl alphanumerische als auch Sonderzeichen und Interpunktionszeichen.
- Ersetzen Sie Buchstaben in einem Kennwort durch Sonderzeichen oder Zahlen. Sie können z. B. die Zahl 1 für den Buchstaben I oder L verwenden.
- Mischen Sie im Kennwort zwei oder mehrere Sprachen.
- Trennen Sie ein Wort oder einen Begriff durch Zahlen oder Sonderzeichen in der Mitte, z. B. „Mary2-2Cat45“.
- Verwenden Sie kein Kennwort, das in einem Wörterbuch vorkommt.
- Benutzen Sie für das Kennwort weder Ihren Namen noch andere persönliche Informationen wie Ihr Geburtsdatum, Namen von Haustieren, Mädchenname der Mutter usw., auch nicht rückwärts geschrieben.
- Ändern Sie das Kennwort regelmäßig. Es genügt, wenn Sie nur einige Zeichen ändern.
- Wenn Sie Ihr Kennwort aufschreiben, bewahren Sie es auf keinen Fall sichtbar in der Nähe des Computers auf.
- Speichern Sie das Kennwort nicht in einer Datei, wie z. B. einer E-Mail, auf dem Computer.
- Nutzen Sie das Konto nicht gemeinsam mit anderen Benutzern, und geben Sie Ihr Kennwort nicht weiter.

Sichern und Wiederherstellen von HP ProtectTools Anmeldedaten

Sie können das Merkmal Sichern und Wiederherstellen von HP ProtectTools verwenden, um HP ProtectTools Anmeldeinformationen und zugehörige Einstellungen auszuwählen und diese zu sichern.

2 Einführung in den Installations-Assistenten

Der Installations-Assistent für Security Manager führt Sie durch den Vorgang zum Aktivieren der Sicherheitsfunktionen, die für alle Benutzer des Computers gelten. Sie können diese Funktionen auch auf der Seite mit den Sicherheitsfunktionen in der Administrator-Konsole verwalten.

So richten Sie im Installations-Assistenten für Security Manager die Sicherheitsfunktionen ein:

1. Öffnen Sie den HP ProtectTools Security Manager über das Symbol der HP ProtectTools Desktop-Minianwendung in der Windows Randleiste oder über das Symbol in der Taskleiste im Infobereich, ganz rechts auf der Taskleiste.

   Die Farbe des Banners der Desktop-Minianwendung HP ProtectTools zeigt eine der folgenden Bedingungen an:

   - Rot – HP ProtectTools wurde nicht eingerichtet, oder eine Fehlerbedingung mit einem der ProtectTools Module liegt vor.
   - Gelb – Auf der Seite für den Status der Anwendungen in Security Manager wird angezeigt, welche Einstellungen geändert werden müssen.
   - Blau – HP ProtectTools wurde eingerichtet und funktioniert ordnungsgemäß.

Wenn eine der folgenden Bedingungen erfüllt ist, wird am unteren Rand des Symbols der Minianwendung eine entsprechende Meldung angezeigt:

- **Jetzt einrichten** – Der Administrator muss auf das Symbol der Minianwendung klicken, um den Security Manager Installations-Assistenten zu starten und Authentifizierungsinformationen für den Computer zu konfigurieren.

  Der Installations-Assistent ist eine eigenständige Anwendung.

- **Jetzt registrieren** – Benutzer müssen auf das Symbol der Minianwendung klicken, um den Security Manager-Einführungsassistenten zu starten und Authentifizierungsinformationen zu registrieren.

  Der Einführungsassistent wird auf dem Security Manager Dashboard angezeigt.

- **Jetzt suchen** – Klicken Sie auf das Symbol der Minianwendung, um weitere Details auf der Seite „Status der Sicherheitsanwendungen" anzeigen zu lassen.

HINWEIS: Die Desktop-Minianwendung HP ProtectTools ist in Windows XP nicht verfügbar.

– ODER –

Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**. Klicken Sie im linken Fensterausschnitt auf **Installations-Assistent**.

2. Lesen Sie den Startbildschirm, und klicken Sie dann auf **Weiter**.

3. Bestätigen Sie Ihre Identität, indem Sie Ihr Windows Kennwort eingeben und anschließend auf **Weiter** klicken.

   Wenn Sie noch kein Windows Kennwort eingerichtet haben, werden Sie aufgefordert, eines einzurichten. Ein Windows Kennwort ist erforderlich, um Ihr Windows Konto vor Zugriffen von unbefugten Personen zu schützen und um die HP ProtectTools Security Manager Funktionen zu verwenden.

4. Wählen Sie auf der SpareKey-Seite drei Sicherheitsfragen aus, geben Sie zu jeder Frage eine Antwort ein, und klicken Sie auf **Weiter**.

   Auf der SpareKey-Seite von **Credential Manager** im Security Manager Dashboard können Sie andere Fragen auswählen bzw. Ihre Antworten ändern.

HINWEIS: Diese SpareKey-Einrichtung ist nur für Administratoren verfügbar.

5. Aktivieren Sie die Sicherheitsfunktionen durch Auswahl der entsprechenden Kontrollkästchen, und klicken Sie dann auf **Weiter**.

   Je mehr Funktionen Sie auswählen, desto sicherer ist Ihr Computer.

HINWEIS: Die hier vorgenommenen Einstellungen gelten für alle Benutzer. Wenn Kontrollkästchen nicht aktiviert sind, wird der Benutzer vom Installations-Assistenten nicht aufgefordert, diese Anmeldedaten zu registrieren.

- **Windows Anmeldesicherheit** – Schützt Ihre Windows Konten, indem es dafür sorgt, dass der Zugriff nur mit bestimmten Anmeldedaten möglich ist.
- **Drive Encryption** schützt Ihre Daten durch die Verschlüsselung Ihrer Festplatten, so dass Informationen für Personen ohne die entsprechende Berechtigung nicht lesbar sind.
- **Pre-Boot Security** schützt Ihren Computer, indem es den Zugriff unbefugter Personen verhindert, bevor Windows gestartet wird.

  HINWEIS: Pre-Boot Security steht nur dann zur Verfügung, wenn diese Funktion vom BIOS unterstützt wird.

6. Sie werden vom Installations-Assistenten aufgefordert, sich zu registrieren oder sich anderweitig zu authentifizieren.

   Wenn weder ein Fingerabdruck-Lesegerät noch eine Smart Card noch eine Webcam zur Verfügung steht, werden Sie aufgefordert, Ihr Windows Kennwort einzugeben. Nach der Registrierung können Sie beliebige registrierte Benutzerdaten verwenden, um bei Bedarf Ihre Identität zu verifizieren.

   HINWEIS: Die Registrierung dieser Anmeldedaten ist nur für Administratoren verfügbar.

7. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

   Die Startseite des Security Manager Dashboard wird angezeigt.

3 HP ProtectTools Security Manager Administrator-Konsole

Die HP ProtectTools Security Manager Software bietet Sicherheitsfunktionen, die den Computer, Netzwerke und wichtige Daten vor unberechtigtem Zugriff schützen. Die Verwaltung von HP ProtectTools Security Manager erfolgt über die Administrator-Konsole.

Im Security Manager Dashboard sind zusätzliche Anwendungen verfügbar (bestimmte Modelle), die Ihnen bei der Wiedererlangung des Computers helfen, falls dieser verloren geht oder gestohlen wird.

Mittels dieser Konsole kann der lokale Administrator die folgenden Aufgaben ausführen:

- Aktivieren oder Deaktivieren von Sicherheitsfunktionen
- Festlegen von erforderlichen Anmeldeinformationen zur Authentifizierung
- Verwalten der Benutzer des Computers
- Anpassen gerätespezifischer Parameter
- Konfigurieren installierter Security Manager Anwendungen
- Hinzufügen von weiteren Security Manager Anwendungen

Öffnen von HP ProtectTools Administrator-Konsole

Für Administrationsaufgaben wie z. B. das Einrichten von Systemrichtlinien oder die Konfiguration von Software öffnen Sie die Konsole folgendermaßen:

▲ Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.

– oder –

Klicken Sie auf der linken Seite von Security Manager auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

Verwenden der Administrator-Konsole

HP ProtectTools Administrator-Konsole ist die zentrale Stelle für die Verwaltung der Funktionen und Anwendungen von HP ProtectTools Security Manager.

▲ Zum Öffnen von HP ProtectTools Administrator-Konsole klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.

  – oder –

  Klicken Sie auf der linken Seite von Security Manager auf **Verwaltung** und anschließend auf **Administrator-Konsole**.

Die Konsole setzt sich aus den folgenden Komponenten zusammen:

- **Startseite** – Hier können Sie die folgenden Sicherheitsoptionen konfigurieren:
  - **Systemsicherheit erhöhen**
  - **Starke Authentifizierung erforderlich**
  - **HP ProtectTools Benutzer verwalten**
  - **Informationen zur zentralen Verwaltung von HP ProtectTools**
- **System** – Ermöglicht die Konfiguration der folgenden Sicherheitsfunktionen und die Authentifizierung für Benutzer und Geräte:
  - **Sicherheit**
  - **Benutzer**
  - **Anmeldeinformationen**
- **Anwendungen** – Ermöglicht die Konfiguration der Einstellungen für HP ProtectTools Security Manager und für Security Manager-Anwendungen.
- **Daten** – Enthält ein erweitertes Menü mit Links zu den Security Manager-Anwendungen, die Ihre Daten schützen.
- **Zentrale Verwaltung** – Zeigt Registerkarten für den Zugriff auf zusätzliche Lösungen, Produktaktualisierungen und Meldungen an.
- **Installations-Assistent** – Führt Sie durch die Installation von HP ProtectTools Security Manager.
- **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.
- **Hauptbereich** – Zeigt anwendungsspezifische Bildschirme an.

  ? – Zeigt Softwarehilfe zur Administrator-Konsole an. Das Hilfe-Symbol befindet sich rechts oben im Fensterrahmen, neben den Symbolen für die Minimierung und Maximierung der Fensteranzeige.

Konfigurieren des Systems

Der Zugriff auf die Gruppe **System** erfolgt über das Menü auf der linken Seite von HP ProtectTools Administrator-Konsole. Mit den Anwendungen aus dieser Gruppe können Sie die Richtlinien und Einstellungen für den Computer sowie die Benutzer und angeschlossenen Geräte verwalten.

Die folgenden Anwendungen sind in der Gruppe **System** enthalten:

- **Sicherheit** – Verwalten von Funktionen, der Authentifizierung und von Einstellungen, die steuern, wie die Benutzer mit diesem Computer interagieren.
- **Benutzer** – Einrichten, Verwalten und Registrieren von Benutzern dieses Computers.
- **Anmeldeinformationen** – Verwalten von Einstellungen für integrierte bzw. an den Computer angeschlossene Sicherheitsgeräte.

Einrichten der Authentifizierung für Ihren Computer

In der Authentifizierungsanwendung können Sie Richtlinien für den Zugriff auf den Computer festlegen. Sie können Anmeldeinformationen festlegen, die für die Authentifizierung jeder Benutzerklasse für die Anmeldung bei Windows oder auf Websites und Programmen während einer Benutzersitzung benötigt werden.

So richten Sie eine Authentifizierung auf Ihrem Computer ein:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Zur Konfiguration der Anmeldeauthentifizierung klicken Sie auf die Registerkarte **Anmelderichtlinie**, nehmen die Änderungen vor und klicken dann auf **Übernehmen**.
3. Zur Konfiguration der Sitzungsauthentifizierung klicken Sie auf die Registerkarte **Sitzungsrichtlinie**, nehmen die Änderungen vor und klicken dann auf **Übernehmen**.

Anmelderichtlinie

So definieren Sie Richtlinien für die Verwaltung der Anmeldedaten, die für die Authentifizierung eines Benutzers bei der Windows Anmeldung erforderlich sind:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Anmelderichtlinie** auf den Pfeil nach unten, und wählen Sie eine Benutzerkategorie:
   - **Für Administratoren dieses Computers**
   - **Für Benutzer ohne Administratorrechte**
3. Geben Sie die für die ausgewählte Benutzerkategorie benötigten Anmeldeinformationen zur Authentifizierung an.
4. Wählen Sie aus, ob EINE BELIEBIGE (nur eine) der angegebenen Anmeldeinformationen erforderlich ist oder ob ALLE angegebenen Anmeldeinformationen für die Authentifizierung eines Benutzers erforderlich sind.
5. Klicken Sie auf **Übernehmen**.

Sitzungsrichtlinie

So bestimmen Sie Richtlinien, die regulieren, welche Anmeldedaten für den Zugriff auf HP ProtectTools Anwendungen in einer Windows Sitzung erforderlich sind:

1. Klicken Sie auf der linken Seite der Administrator-Konsole auf **Sicherheit** und anschließend auf **Authentifizierung**.
2. Klicken Sie auf der Registerkarte **Sitzungsrichtlinie** auf den Pfeil nach unten, und wählen Sie eine Benutzerkategorie:
   - **Für Administratoren dieses Computers**
   - **Für Benutzer ohne Administratorrechte**
3. Klicken Sie auf den Pfeil nach unten, und wählen Sie die erforderlichen Authentifizierungsinformationen für die gewählte Benutzerkategorie aus:
   - **Eine der angegebenen Anmeldeinformationen ist erforderlich**

     HINWEIS: Das Deaktivieren der Kontrollkästchen für alle Anmeldeinformationen hat dieselbe Wirkung wie das Auswählen der Option **Authentifizierung ist nicht erforderlich**.
   - **Alle der angegebenen Anmeldeinformationen sind erforderlich**
   - **Authentifizierung ist nicht erforderlich** – Bei Auswahl dieser Option werden alle Anmeldeinformationen aus dem Fenster gelöscht.
4. Klicken Sie auf **Übernehmen**.

Einstellungen

1. Zum Aktivieren/Deaktivieren der folgenden Einstellung verwenden Sie das entsprechende Kontrollkästchen.

   One-Step Logon zulassen – Ermöglicht es den Benutzern dieses Computers, die Windows Anmeldung zu überspringen, wenn die Authentifizierung im BIOS oder über eine verschlüsselte Festplatte erfolgt ist.
2. Klicken Sie auf **Übernehmen**.

Verwalten von Benutzern

In der Anwendung „Benutzer" können Sie die HP ProtectTools Benutzer dieses Computers überwachen und verwalten.

Alle HP ProtectTools Benutzer werden aufgeführt, und es wird geprüft, ob Sie die Richtlinien von Security Manager erfüllen und ob sie die richtigen Anmeldedaten registriert haben, die es ihnen ermöglichen, diese Richtlinien einzuhalten.

Zum Verwalten von Benutzern wählen Sie die folgenden Einstellungen aus:

- Um weitere Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen**.
- Um einen Benutzer zu löschen, klicken Sie auf den Benutzer und danach auf **Löschen**.

- Um zusätzliche Anmeldeinformationen für den Benutzer einzurichten, klicken Sie auf **Registrieren**.
- Um die Richtlinien für einen bestimmten Benutzer anzuzeigen, wählen Sie den Benutzer aus. Die Richtlinien werden dann im unteren Fenster angezeigt.

Anmeldeinformationen

In der Anwendung „Anmeldeinformationen“ können Sie Einstellungen für integrierte oder angeschlossene Sicherheitsgeräte, die von HP ProtectTools Security Manager erkannt werden, festlegen.

SpareKey

Sie können einstellen, ob Sie die SpareKey-Authentifizierung für die Windows Anmeldung zulassen möchten oder nicht, und die Sicherheitsfragen verwalten, die den Benutzern bei der SpareKey-Anmeldung gestellt werden.

1. Aktivieren oder deaktivieren Sie das Kontrollkästchen, um die SpareKey-Authentifizierung für die Windows Anmeldung zu aktivieren oder zu deaktivieren.
2. Wählen Sie die Sicherheitsfragen aus, die den Benutzern bei der SpareKey-Anmeldung gestellt werden. Sie können bis zu drei benutzerdefinierte Fragen angeben, oder Sie können Benutzern ermöglichen, ihre eigene Passphrase einzugeben.
3. Klicken Sie auf **Übernehmen**.

Fingerabdrücke

Wenn der Computer über ein integriertes oder angeschlossenes Fingerabdruck-Lesegerät verfügt, werden auf der Seite „Fingerabdrücke“ folgende Registerkarten angezeigt:

- **Registrierung** – Wählen Sie die Mindest- und die Maximalanzahl an Fingerabdrücken, die ein Benutzer registrieren kann.

  Sie können ebenfalls alle Daten vom Fingerabdruck-Lesegerät löschen.

  ACHTUNG: Wenn Sie alle Daten aus dem Fingerabduck-Lesegerät löschen, werden die Fingerabdruckdaten aller Benutzer gelöscht, einschließlich des Administrators. Falls die Anmelderichtlinie nur die Authentifizierung per Fingerabdruck vorsieht, kann dies dazu führen, dass sich keiner der Benutzer mehr an diesem Computer anmelden kann.

- **Empfindlichkeit** – Bewegen Sie den Schieberegler, um die Empfindlichkeit des Fingerabdruck-Lesegeräts anzupassen, mit der Fingerabdrücke beim Streichen über den Sensor erkannt werden.

  Wenn Ihr Fingerabdruck nicht konsistent erkannt wird, müssen Sie ggf. die Empfindlichkeit vermindern. Eine höhere Einstellung erhöht die Empfindlichkeit für Abweichungen bei der Registrierung von Fingerabdrücken durch Streichen über den Sensor und verringert dadurch die Möglichkeit eines fälschlicherweise zugelassenen Zugriffs. Die Einstellung **Mittel-hoch** bietet eine gute Mischung aus Sicherheit und Komfort.

- **Erweitert** – Wählen Sie eine der folgenden Optionen, um das Fingerabdruck-Lesegerät so zu konfigurieren, dass Strom gespart und Bildschirmmeldungen verbessert werden:
  - **Optimiert** – Das Fingerabdruck-Lesegerät wird aktiviert, wenn es benötigt wird. Bei der ersten Verwendung des Geräts kann es zu einer leichten Verzögerung kommen.
  - **Geringer Stromverbrauch** – Das Fingerabdruck-Lesegerät reagiert langsamer, bei dieser Einstellung wird jedoch deutlich weniger Strom benötigt.
  - **Normaler Stromverbrauch** – Das Fingerabdruck-Lesegerät ist jederzeit einsatzbereit, bei dieser Einstellung wird jedoch am meisten Strom benötigt.

Smart Card

Wenn der Computer über ein integriertes oder angeschlossenes Lesegerät für Smart Cards verfügt, werden auf der Seite „Smart Card“ folgende Registerkarten angezeigt:

- **Einstellungen** – Sie können den Computer so einstellen, dass er beim Entfernen einer Smart Card automatisch gesperrt wird.

  HINWEIS: Der Computer wird jedoch nur dann gesperrt, wenn die Smart Card als Anmeldeinformation zur Authentifizierung bei der Windows Anmeldung genutzt wurde. Wenn eine Smart Card entfernt wird, die nicht für die Windows Anmeldung verwendet wurde, wird der Computer nicht gesperrt.

- **Verwaltung** – Wählen Sie eine der folgenden Optionen:
  - **Initialize the smart card** (Smart Card initialisieren) – Bereitet eine Smart Card für die Verwendung mit HP Protect Tools vor. Wenn eine Smart Card zuvor bereits außerhalb von HP ProtectTools initialisiert wurde (und ein asymmetrisches Schlüsselpaar sowie das zugehörige Zertifikat enthält), muss sie nicht erneut initialisiert werden, es sei denn, es wird eine Initialisierung mit einem bestimmten Zertifikat gewünscht.
  - **Change smart card PIN** (Smart Card-PIN ändern) – Hiermit können Sie die mit der Smart Card verwendete PIN ändern.
  - **Erase HP ProtectTools data only** (Nur HP ProtectTools Daten löschen) – Löscht nur das während der Karteninitialisierung erstellte HP ProtectTools Zertifikat. Es werden keine anderen Daten von der Karte gelöscht.
  - **Erase all data on the smart card** (Alle Daten von der Smart Card löschen) – Löscht alle Daten von der angegebenen Smart Card. Die Karte kann dann nicht mehr mit HP ProtectTools oder anderen Anwendungen verwendet werden.



HINWEIS: Funktionen, die von Ihrer Smart Card nicht unterstützt werden, sind nicht verfügbar.

▲ Klicken Sie auf **Übernehmen**.

Gesicht

Wenn der Computer über eine integrierte oder angeschlossene Webcam verfügt, und wenn das Gesichtserkennungsprogramm installiert ist, können Sie die Sicherheitsstufe für die Gesichtserkennung so einstellen, dass ein Gleichgewicht zwischen Nutzungskomfort und Computersicherheit hergestellt wird.

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie auf **Anmeldeinformationen** und dann auf **Gesicht**.

3. Für mehr Komfort bewegen Sie den Schieberegler nach links, für mehr Genauigkeit bewegen Sie den Schieberegler nach rechts.

   - **Komfort** – Um registrierten Benutzern den Zugriff in Grenzsituationen zu erleichtern, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Komfort**.

   - **Balance** – Um ein gutes Gleichgewicht zwischen Sicherheit und Komfort herzustellen, oder wenn auf dem Computer kritische Informationen gespeichert sind bzw. sich der Computer in einer Umgebung befindet, in der unberechtigte Anmeldeversuche möglich sind, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Balance**.

   - **Genauigkeit** – Um den Zugriff für Benutzer zu erschweren, wenn die registrierten Szenen oder aktuellen Lichtbedingungen unter dem Normalwert liegen und fälschlicherweise zugelassene Zugriffe möglich sind, klicken Sie auf den Schieberegler, und bewegen Sie ihn zur Position **Genauigkeit**.

4. Klicken Sie auf **Erweitert**, und konfigurieren Sie zusätzliche Sicherheitsoptionen. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen“ auf Seite 46.

5. Klicken Sie auf **Übernehmen**.

Konfigurieren der Anwendungen

Sie können die Einstellungen nutzen, um das Verhalten der installierten HP ProtectTools Security Manager Anwendungen anzupassen.

So bearbeiten Sie die Anwendungseinstellungen:

1. Klicken Sie auf der linken Seite der Administrator-Konsole unter **Anwendungen** auf **Einstellungen**.
2. Zum Aktivieren/Deaktivieren einer bestimmten Einstellung verwenden Sie das entsprechende Kontrollkästchen.
3. Klicken Sie auf **Übernehmen**.

Registerkarte „Allgemein“

Die folgenden Einstellungen stehen auf der Registerkarte **Allgemein** zur Verfügung:

- **Installations-Assistent für Administratoren nicht automatisch starten** – Wählen Sie diese Option aus, um zu verhindern, dass der Assistent automatisch bei der Anmeldung geöffnet wird.
- **Einführungsassistent für Benutzer nicht automatisch starten** – Wählen Sie diese Option, um zu verhindern, dass die Benutzerinstallation automatisch bei der Anmeldung geöffnet wird.

Registerkarte „Anwendungen”

Die hier dargestellten Einstellungen können sich ändern, wenn neue Anwendungen zu Security Manager hinzugefügt werden. Standardmäßig werden jedoch mindestens die folgenden Einstellungen angezeigt:

- **Status der Anwendungen** – Aktiviert die Anzeige des Status für alle Anwendungen.
- **Password Manager** – Aktiviert den Password Manager für alle Benutzer des Computers.
- **Privacy Manager** – Aktiviert den Privacy Manager für alle Benutzer des Computers.
- **Verknüpfung für zentrale Verwaltung aktivieren** – Ermöglicht es allen Benutzern dieses Computers, Anwendungen zu HP ProtectTools Security Manager hinzuzufügen, indem sie auf die Schaltfläche **Zentrale Verwaltung** klicken.

Um alle Anwendungen auf die Werkseinstellung zurückzusetzen, klicken Sie auf die Schaltfläche **Standardeinstellungen wiederherstellen**.

Zentrale Verwaltung

Möglicherweise sind zusätzliche Anwendungen verfügbar, um neue Management-Tools in Security Manager aufzunehmen. Der Administrator dieses Computers kann diese Funktion auf der Seite „Einstellungen“ deaktivieren. Auf der Seite „Zentrale Verwaltung“ befinden sich zwei Registerkarten:

- **Unternehmenslösungen** – Falls eine Internetverbindung verfügbar ist, können Sie auf der DigitalPersona Website (http://www.digitalpersona.com/) nach neuen Anwendungen suchen.
- **Updates und Nachrichten**
  - Um Informationen zu neuen Anwendungen und Updates anzufordern, aktivieren Sie das Kontrollkästchen **Über neue Anwendungen und Updates informieren**.
  - Zum Einrichten eines Zeitplans für automatische Updates wählen Sie die Anzahl der Tage.
  - Zum Suchen nach Updates klicken Sie auf **Jetzt suchen**.

4 HP ProtectTools Security Manager

HP ProtectTools Security Manager ermöglicht Ihnen, die Sicherheit Ihres Computers beträchtlich zu erhöhen.

Sie können vorinstallierte Security Manager Anwendungen sowie zusätzliche Anwendungen nutzen, die zum sofortigen Download aus dem Internet zur Verfügung stehen:

- Benutzernamen und Kennwörter verwalten.
- Kennwort für das Windows® Betriebssystem schnell und einfach ändern.
- Programmeinstellungen festlegen.
- Fingerabdrücke für zusätzliche Sicherheit und gesteigerten Komfort verwenden.
- Eine oder mehrere Szenen für die Authentifizierung registrieren.
- Eine Smart Card zur Authentifizierung einrichten.
- Programmdaten sichern und wiederherstellen.
- Weitere Anwendungen hinzufügen.

Öffnen von Security Manager

Security Manager lässt sich auf folgende Arten starten:

- Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
- Doppelklicken Sie auf das Symbol **HP ProtectTools** im Infobereich außen rechts in der Taskleiste.
- Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** und anschließend auf **HP ProtectTools Security Manager öffnen**.
- Klicken Sie auf die Desktop-Minianwendung **HP ProtectTools**.
- Drücken Sie die Tastenkombination strg+Windows Logo-Taste+h, um das Menü **Security Manager Quick Links** (Security Manager Verknüpfungen) zu öffnen.

  Weitere Informationen zum Ändern der Tastenkombination finden Sie unter „Einstellungen“ auf Seite 40.

Verwenden des Security Manager Dashboards

Das Security Manager Dashboard ist die zentrale Zugriffsstelle auf die Funktionen, Anwendungen und Einstellungen von Security Manager.

▲ Zum Öffnen des Security Manager Dashboards klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.

Das Dashboard enthält die folgenden Komponenten:

- **ID-Card** – Zeigt den Windows Benutzernamen und ein ausgewähltes Bild zur Ermittlung des angemeldeten Benutzerkontos an.
- **Sicherheitsanwendungen** – Zeigt ein erweitertes Menü mit Links an, über die folgende Sicherheitskategorien konfiguriert werden können:
  - **Startseite** – Ermöglicht die Verwaltung von Kennwörtern, die Einrichtung von Authentifizierungsinformationen und die Überprüfung des Status der Sicherheitsanwendungen.
  - **Status** – Ermöglicht die Überprüfung des Status der HP ProtectTools Sicherheitsanwendungen.

HINWEIS: Nicht auf dem Computer installierte Anwendungen werden in der folgenden Liste nicht aufgeführt.

- **My Logons** (Meine Anmeldedaten) – Ermöglicht die Verwaltung der verschiedenen Authentifizierungsinformationen (Password Manager, Credential Manager, Kennwort, SpareKey, Smart Card, Gesichtserkennung, Fingerabdruck).
- **Meine Daten** – Ermöglicht die Verwaltung der Datensicherheit mit Drive Encryption und File Sanitizer.
- **Arbeitsplatz** – Ermöglicht die Verwaltung der Sicherheit Ihres Computers mit Device Access Manager.
- **Meine Kommunikation** – Ermöglicht die Verwaltung der Kommunikationssicherheit mit Privacy Manager.
- **Verwaltung** – Ermöglicht Administratoren den Zugriff auf folgende Optionen:
  - **Administrator-Konsole** – Ermöglicht Administratoren die Verwaltung von Sicherheit und Benutzern.
  - **Zentrale Verwaltung** – Ermöglicht Administratoren des Zugriff auf zusätzliche Lösungen, Produktaktualisierungen und Meldungen.
- **Erweitert** – Enthält Befehle für den Zugriff auf zusätzliche Funktionen, wie beispielsweise:
  - **Voreinstellungen** – Ermöglicht die Personalisierung der Security Manager Einstellungen.
  - **Sichern und Wiederherstellen** – Ermöglicht die Sicherung und Wiederherstellung von Daten.
  - **Info** – Zeigt Informationen zu HP ProtectTools Security Manager, wie etwa Versionsnummer und Copyright-Hinweis, an.

- **Hauptbereich** – Zeigt anwendungsspezifische Bildschirme an.
- **?** – Öffnet die Softwarehilfe zu Security Manager. Das Hilfe-Symbol befindet sich rechts oben im Fenster, neben den Symbolen für die Minimierung und Maximierung der Fensteranzeige.

Status der Sicherheitsanwendungen

Der Status Ihrer installierten Sicherheitsanwendungen wird an zwei Stellen angezeigt:

- In der **HP ProtectTools Desktop-Minianwendung**

  Die Farbe des Banners ganz oben im Symbol der HP ProtectTools Minianwendung ändert sich je nach Gesamtstatus der installierten Sicherheitsanwendungen.

  - **Rot** – Vorsicht
  - **Gelb** – Achtung: nicht konfiguriert
  - **Blau** – OK

  Wenn eine der folgenden Bedingungen erfüllt ist, wird am unteren Rand des Symbols der Minianwendung eine entsprechende Meldung angezeigt:

  - **Jetzt einrichten** – Der Administrator muss auf das Symbol der Minianwendung klicken, um den Security Manager Installations-Assistenten zu starten und Authentifizierungsinformationen für den Computer zu konfigurieren.

    Der Installations-Assistent ist eine eigenständige Anwendung.
  - **Jetzt registrieren** – Benutzer müssen auf das Symbol der Minianwendung klicken, um den Security Manager-Einführungsassistenten zu starten und Authentifizierungsinformationen zu registrieren.

    Der Einführungsassistent wird auf dem Security Manager Dashboard angezeigt.
  - **Jetzt suchen** – Klicken Sie auf das Symbol der Minianwendung, um weitere Details auf der Seite „Status der Sicherheitsanwendungen“ anzuzeigen.
- Seite **Status der Sicherheitsanwendungen** – Klicken Sie im Security Manager Dashboard auf **Status**, um den Gesamtstatus Ihrer installierten Sicherheitsanwendungen sowie den Status der einzelnen Anwendungen anzuzeigen.

My Logons (Meine Anmeldedaten)

Die in dieser Gruppe enthaltenen Anwendungen unterstützen Sie bei der Verwaltung verschiedener Aspekte Ihrer digitalen Identität.

- **Password Manager** – Erstellt und verwaltet Verknüpfungen, über die Sie Websites und Programme starten und sich bei diesen anmelden können, indem Sie sich mit Ihrem Windows Kennwort, Ihrem Fingerabdruck oder einer Smart Card authentifizieren.
- **Credential Manager** – Hier können Sie ganz einfach Ihr Windows Kennwort ändern, Ihre Fingerabdrücke registrieren oder eine Smart Card einrichten.

Administratoren können weitere Anwendungen hinzufügen, indem Sie auf **Verwaltung** und anschließend auf **Zentrale Verwaltung** links unten im Dashboard klicken.

Password Manager

Mit Password Manager wird das Anmelden bei Windows, Websites und Anwendungen einfacher und sicherer. Sie können dieses Tool verwenden, um Kennwörter mit höherer Sicherheit zu erstellen, die Sie nicht aufschreiben oder im Kopf behalten müssen. Sie können sich dann schnell und einfach per Fingerabdruck, Smart Card oder mit Ihrem Windows Kennwort anmelden.

Password Manager bietet folgende Optionen:

- Hinzufügen, Bearbeiten oder Löschen von Anmeldedaten über die Registerkarte **Verwalten**.
- Verwenden von Verknüfungen zum Starten Ihres Standardbrowsers und Anmelden bei beliebigen Websites oder Programmen (nach entsprechender Einrichtung).
- Verschieben von Verknüpfungen per Drag and Drop, um diese nach Belieben in Kategorien einzuordnen.
- Auf einen Blick erkennen, ob eines Ihrer Kennwörter ein Sicherheitsrisiko birgt, und automatisch komplexe Kennwörter mit hoher Sicherheit für neue Websites generieren.

Das **Password Manager**-Symbol befindet sich links oben auf einer Webseite oder dem Anmeldebildschirm einer Anwendung. Wenn noch keine Anmeldedaten für die Website oder Anwendung festgelegt wurden, enthält das Symbol ein Pluszeichen.

▲ Klicken Sie auf das **Password Manager**-Symbol, um ein Kontextmenü anzuzeigen, in dem Sie aus den im Folgenden genannten Optionen wählen können.

Für Webseiten oder Programme, für die noch keine Anmeldedaten festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **[beliebigeDomäne.de] zu Password Manager hinzufügen** – Ermöglicht das Hinzufügen von Anmeldedaten für den aktuellen Anmeldebildschirm.
- **Password Manager öffnen** – Startet Password Manager.
- **Symboleinstellungen** – Hier können Sie Bedingungen festlegen, unter denen das **Password Manager**-Symbol angezeigt werden soll.
- **Hilfe** – Öffnet die Softwarehilfe zu Security Manager.

Für Webseiten oder Programme, für die bereits Anmeldedaten festgelegt wurden

Folgende Optionen werden im Kontextmenü angezeigt:

- **Anmeldedaten eingeben** – Fügt Ihre Anmeldedaten in die Anmeldefelder ein und sendet sie an die Seite (wenn das Senden beim Erstellen oder bei der letzten Änderung der Anmeldedaten festgelegt wurde).
- **Anmeldedaten bearbeiten** – Hier können Sie Ihre Anmeldedaten für diese Website bearbeiten.
- **Anmeldedaten hinzufügen** – Hier können Sie ein Konto zu Anmeldedaten hinzufügen.
- **Password Manager öffnen** – Startet Password Manager.
- **Hilfe** – Öffnet die Softwarehilfe zu Security Manager.

HINWEIS: Möglicherweise hat der Administrator dieses Computers Security Manager so eingerichtet, dass mehr als eine Authentifizierung zur Verifizierung Ihrer Identität erforderlich ist.

Hinzufügen von Anmeldedaten

Sie können ganz einfach Anmeldedaten für eine Website oder ein Programm hinzufügen, indem Sie diese einmal eingeben. Ab diesem Zeitpunkt gibt Password Manager diese Daten automatisch für Sie ein. Sie können diese Anmeldedaten verwenden, nachdem Sie zur entsprechenden Website oder dem Programm navigiert sind, oder indem Sie im Menü **Anmeldedaten** auf bestimmte Anmeldedaten klicken, woraufhin Password Manager die Website oder das Programm für Sie öffnet und die Anmeldung vornimmt.

So fügen Sie Anmeldedaten hinzu:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.
2. Klicken Sie auf den Pfeil am **Password Manager**-Symbol, und klicken Sie dann auf eine der folgenden Optionen, je nachdem, ob es sich um den Anmeldebildschirm einer Website oder eines Programms handelt.
   - Klicken Sie im Falle einer Website auf **[Domänenname] zu Password Manager hinzufügen**.
   - Klicken Sie im Falle eines Programms auf **Diesen Anmeldebildschirm zu Password Manager hinzufügen**.
3. Geben Sie Ihre Anmeldedaten ein. Anmeldefelder auf dem Bildschirm und ihre entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangefarbenen Umrandung gekennzeichnet. Sie können dieses Dialogfeld auch anzeigen, indem Sie auf der Registerkarte **Verwalten** von Password Manager auf **Anmeldedaten hinzufügen** klicken. Bei einigen Optionen kommt es darauf an, welche Sicherheitsgeräte an den Computer angeschlossen sind; dies gilt z. B. für die Tastenkombination strg+Windows Logo-Taste+h, das Streichen mit dem Finger über den Sensor oder das Einsetzen einer Smart Card.
   a. Um ein Anmeldefeld mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf die Pfeile rechts vom Feld.
   b. Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.
   c. Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten automatisch senden**.

d. Zur Aktivierung der VeriSign VIP-Sicherheit aktivieren Sie das Kontrollkästchen **I want VIP security on this site** (Ich möchte VIP-Sicherheit auf dieser Website).

   Diese Option wird nur auf Websites angezeigt, die die VeriSign Identity Protection (VIP)-Funktion unterstützen. Wenn die VIP-Sicherheit von der betreffenden Website unterstützt wird, können Sie zudem festlegen, dass zusätzlich zur üblichen Authentifizierungsmethode auch Ihr VIP-Sicherheitscode eingegeben wird.

e. Klicken Sie auf **OK** und anschließend auf die gewünschte Authentifizierungsmethode (Fingerabdruck, Kennwort, Gesichtserkennung). Melden Sie sich dann mit dieser Methode an.

   Das Pluszeichen wird aus dem **Password Manager**-Symbol entfernt, um anzugeben, dass die Anmeldedaten erstellt wurden.

f. Falls Password Manager die Anmeldedaten nicht erkennt, klicken Sie auf **Weitere Felder**.

   - Aktivieren Sie das Kontrollkästchen für jedes Feld, das für die Anmeldung erforderlich ist, oder deaktivieren Sie das Kontrollkästchen für alle Felder, die nicht für die Anmeldung erforderlich sind.
   - Wenn Password Manager nicht alle Anmeldefelder erkennen kann, werden Sie gefragt, ob Sie fortfahren möchten. Klicken Sie auf **Ja**.
   - Ein Dialogfeld mit Ihren Anmeldedaten wird angezeigt. Klicken Sie auf das Symbol für jedes Feld, und ziehen Sie es zum entsprechenden Anmeldefeld. Klicken Sie anschließend auf die Schaltfläche, um sich bei der Website anzumelden.

     HINWEIS: Wenn Sie sich einmal für die Verwendung des manuellen Modus entschieden haben, um Anmeldedaten für eine Website einzugeben, müssen Sie diese Methode auch für künftige Anmeldungen bei dieser Website verwenden.

     HINWEIS: Der manuelle Modus zur Eingabe von Anmeldedaten ist nur in Verbindung mit Internet Explorer 8 verfügbar.

   - Klicken Sie auf **Schließen**.

Bei jedem Aufrufen dieser Website oder dieses Programms wird das **Password Manager**-Symbol links oben auf der Website bzw. dem Anmeldebildschirm der Anwendung angezeigt. Es gibt an, dass Sie Ihre registrierten Anmeldedaten für die Anmeldung verwenden können.

Bearbeiten von Anmeldedaten

Gehen Sie folgendermaßen vor, um Anmeldedaten zu bearbeiten:

1. Öffnen Sie den Anmeldebildschirm für eine Website oder ein Programm.

2. Um ein Dialogfeld anzuzeigen, in dem Sie Ihre Anmeldedaten bearbeiten können, klicken Sie auf den Pfeil auf dem **Password Manager**-Symbol und anschließend auf **Anmeldedaten bearbeiten**. Anmeldefelder auf dem Bildschirm und ihre entsprechenden Felder im Dialogfeld sind mit einer fett formatierten orangen Umrandung gekennzeichnet.

   Sie können dieses Dialogfeld auch anzeigen, indem Sie auf der Registerkarte **Verwalten** im **Password Manager** auf **Für gewünschte Anmeldedaten bearbeiten** klicken.

3. Bearbeiten Sie Ihre Anmeldedaten.
   - Um ein Anmeldefeld **Benutzername** mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf den Abwärtspfeil rechts von dem Feld.
   - Um ein Anmeldefeld **Kennwort** mit einer der vorformatierten Auswahlmöglichkeiten zu füllen, klicken Sie auf den Abwärtspfeil rechts von dem Feld.
   - Zur Aktivierung der VeriSign VIP-Sicherheit aktivieren Sie das Kontrollkästchen **I want VIP security on this site** (Ich möchte VIP-Sicherheit auf dieser Website).

     Diese Option wird nur auf Websites angezeigt, die die VeriSign VIP-Funktion unterstützen. Wenn die VIP-Sicherheit von der betreffenden Website unterstützt wird, können Sie zudem festlegen, dass zusätzlich zur üblichen Authentifizierungsmethode auch Ihr VIP-Sicherheitscode eingegeben wird.
   - Um weitere Felder vom Bildschirm zu Ihren Anmeldedaten hinzuzufügen, klicken Sie auf **Weitere Felder**.
   - Um das Kennwort für diese Anmeldedaten anzuzeigen, klicken Sie auf **Kennwort einblenden**.
   - Um die Anmeldefelder automatisch auszufüllen, jedoch nicht zu senden, deaktivieren Sie das Kontrollkästchen **Anmeldedaten automatisch senden**.
4. Klicken Sie auf **OK**.

Verwenden des Menüs „Anmeldedaten“

Password Manager ermöglicht es Ihnen, auf schnelle und einfache Art Websites und Programme zu starten, für die Sie Anmeldedaten festgelegt haben. Doppelklicken Sie im Menü **Anmeldedaten** oder auf der Registerkarte **Verwalten** von Password Manager auf die Anmeldedaten für ein Programm oder eine Website, um den Anmeldebildschirm zu öffnen, und geben Sie dann Ihre Anmeldedaten ein.

Wenn Sie Anmeldedaten festlegen, werden diese automatisch in das Menü **Anmeldedaten** von Password Manager übernommen.

So zeigen Sie das Menü **Anmeldedaten** an:

1. Drücken Sie die Tastenkombination für **Password Manager** (die Werkseinstellung lautet strg +Windows Logo-Taste+h). Zum Ändern der Tastenkombination klicken Sie im Security Manager Dashboard auf **Password Manager** und anschließend auf **Einstellungen**.
2. Streichen Sie mit Ihrem Finger über den Sensor (bei Computern mit integriertem oder angeschlossenem Fingerabdruck-Lesegerät), oder geben Sie Ihr Windows Kennwort ein.

Organisieren von Anmeldedaten in Kategorien

Erstellen Sie zum Ordnen Ihrer Anmeldedaten eine oder mehrere Kategorien. Verschieben Sie dann die Anmeldedaten per Drag & Drop in die gewünschten Kategorien.

So fügen Sie eine Kategorie hinzu:

1. Klicken Sie im Security Manager Dashboard auf **Password Manager**.
2. Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Kategorie hinzufügen**.

3. Geben Sie einen Namen für die Kategorie ein.
4. Klicken Sie auf **OK**.

So fügen Sie Anmeldedaten einer Kategorie hinzu:

1. Platzieren Sie den Mauszeiger über den gewünschten Anmeldedaten.
2. Halten Sie die linke Maustaste gedrückt.
3. Ziehen Sie die Anmeldedaten in die Liste der Kategorien. Die Kategorien werden hervorgehoben, wenn Sie den Mauszeiger darüber bewegen.
4. Lassen Sie die Maustaste los, wenn die gewünschte Kategorie hervorgehoben wird.

Ihre Anmeldedaten werden nicht in die ausgewählte Kategorie verschoben, sondern lediglich dorthin kopiert. Sie können dieselben Anmeldedaten zu mehreren Kategorien hinzufügen und alle Ihre Anmeldedaten anzeigen, indem Sie auf **Alle** klicken.

Verwalten Ihrer Anmeldedaten

Mit Password Manager können Sie ganz einfach Ihre Anmeldedaten für Benutzernamen, Kennwörter und mehrere Anmeldekonten von einer zentralen Stelle aus verwalten.

Ihre Anmeldedaten werden auf der Registerkarte **Verwalten** aufgeführt. Wenn mehrere Anmeldedaten für dieselbe Website erstellt wurden, werden die einzelnen Anmeldedaten unter dem Website-Namen aufgelistet und in der Anmeldeliste eingerückt.

So verwalten Sie Ihre Anmeldedaten:

▲ Klicken Sie im Security Manager-Dashboard auf **Password Manager** und anschließend auf die Registerkarte **Verwalten**.

- **Anmeldedaten hinzufügen** – Klicken Sie auf **Anmeldedaten hinzufügen**, und folgen Sie den Anleitungen auf dem Bildschirm.
- **Ihre Anmeldedaten** – Klicken Sie auf vorhandene Anmeldedaten, wählen Sie eine der folgenden Optionen aus, und folgen Sie dann den Anleitungen auf dem Bildschirm:
  - **Öffnen** – Öffnet eine Website oder ein Programm, für die/das Sie Anmeldedaten erstellt haben.
  - **Hinzufügen** – Fügt Anmeldedaten hinzu. Weitere Informationen finden Sie unter „Hinzufügen von Anmeldedaten“ auf Seite 34.
  - **Bearbeiten** – Ermöglicht die Bearbeitung von Anmeldedaten. Weitere Informationen finden Sie unter „Bearbeiten von Anmeldedaten“ auf Seite 35.
  - **Löschen** – Löscht eine Website oder ein Programm, für die/das Sie Anmeldedaten festgelegt haben.
- **Kategorie hinzufügen** – Klicken Sie auf **Kategorie hinzufügen**, und folgen Sie dann den Anleitungen auf dem Bildschirm. Weitere Informationen finden Sie unter „Organisieren von Anmeldedaten in Kategorien“ auf Seite 36.

So fügen Sie zusätzliche Anmeldedaten für eine Website oder ein Programm hinzu:

1. Öffnen Sie den Anmeldebildschirm für die Website oder das Programm.
2. Klicken Sie auf das **Password Manager**-Symbol, um das Kontextmenü anzuzeigen.
3. Klicken Sie auf **Anmeldedaten hinzufügen**, und folgen Sie dann den Anleitungen auf dem Bildschirm.

Einschätzen der Kennwortsicherheit

Das Verwenden von Kennwörtern mit hoher Sicherheit für die Anmeldung bei Ihren Programmen und Websites stellt einen wichtigen Aspekt beim Schutz Ihrer Identität dar.

Password Manager analysiert sofort und automatisch die Sicherheit der Kennwörter, die Sie zum Anmelden bei Websites und Programmen verwenden, und ermöglicht auf diese Weise eine einfache Überwachung und Verbesserung Ihrer Sicherheit.

Einstellungen für das Password Manager Symbol

Password Manager versucht, Anmeldebildschirme für Websites und Programme zu identifizieren. Wenn ein Anmeldebildschirm erkannt wird, für den Sie noch keine Anmeldedaten erstellt haben, fordert Sie Password Manager auf, Anmeldedaten für diesen Bildschirm zu erstellen, indem das **Password Manager**-Symbol mit einem Pluszeichen angezeigt wird.

1. Klicken Sie auf das Pfeilsymbol und anschließend auf **Symboleinstellungen**, um festzulegen, wie Password Manager mögliche Anmelde-Sites behandelt.

   - **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern** – Klicken Sie auf diese Option, wenn Sie möchten, dass Password Manager Sie zum Erstellen von Benutzerdaten auffordert, wenn ein Anmeldebildschirm angezeigt wird, für den noch keine Anmeldedaten eingerichtet sind.

   - **Diesen Bildschirm ausschließen** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht erneut von Password Manager aufgefordert werden möchten, Anmeldedaten für diesen Anmeldebildschirm hinzuzufügen.

     So fügen Sie Anmeldedaten für einen neuen Bildschirm hinzu:

     - Öffnen Sie den Website-Anmeldebildschirm oder die Programmseite, für die noch keine Anmeldedaten eingerichtet wurden; öffnen Sie dann das Security Manager Dashboard, und klicken Sie auf **Password Manager**.

     - Klicken Sie auf **Anmeldedaten hinzufügen**.

       Das Dialogfeld „Anmeldedaten hinzufügen“ wird geöffnet, wobei der Anmeldebildschirm für die Website oder das Programm im Feld **Current screen** (Aktueller Bildschirm) aufgeführt wird.

     - Klicken Sie auf **Weiter**.

       Der Bildschirm „Anmeldedaten zu Password Manager hinzufügen“ wird angezeigt.

   - Folgen Sie den Anleitungen auf dem Bildschirm. Weitere Informationen finden Sie unter „Hinzufügen von Anmeldedaten“ auf Seite 34.
   - Das **Password Manager**-Symbol wird bei nun jedem Öffnen dieses Website-Anmeldebildschirms bzw. Programmbildschirms angezeigt.

2. Wenn keine Aufforderung zum Hinzufügen von Anmeldedaten angezeigt werden soll, deaktivieren Sie das betreffende Kontrollkästchen.

3. Für den Zugriff auf weitere Password Manager-Einstellungen klicken Sie auf **Password Manager** und anschließend im Security Manager-Dashboard auf **Einstellungen**.

VeriSign Identity Protection (VIP)

Für Websites, die die VeriSign VIP-Funktion unterstützen, können Sie VeriSign VIP-Zugriffstoken erzeugen. Anhand dieser Token erstellt Password Manager automatische Anmeldedaten, bei denen die Token mittels Drag & Drop in Anmeldebildschirme mit VeriSign VIP-Unterstützung übernommen bzw. von Hand in vorgegebene Felder eingegeben werden.

Die Aktivierung der VeriSign VIP-Funktion und die Erzeugung eines Tokens kann im Security Manager Dashboard oder auf einer beliebigen Website mit VeriSign VIP-Unterstützung vorgenommen werden. Zur Verwendung des Tokens müssen Sie sich auf jeder Website registrieren, auf der das Token genutzt werden soll.

Nach der Registrierung und vor dem ersten Gebrauch können Sie das Token (optional) an Ihre regulären Anmeldedaten koppelt und mit diesen verwenden. Falls die betreffende Website eine Koppelung der Anmeldedaten mit einem Token nicht zulässt, können Sie die Token-Daten auch manuell in das betreffende Feld ziehen und dort ablegen.

So aktivieren Sie VeriSign VIP und erzeugen ein VeriSign VIP-Token im Security Manager Dashboard:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 29.

2. Klicken Sie auf **Password Manager** und anschließend auf **VIP**.

3. Klicken Sie auf **Get VIP** (VIP abrufen).

   Ein VeriSign VIP-Token wird erzeugt und auf der VeriSign VIP-Seite angezeigt. Das Token wird nun bei jedem Zugriff auf diese Seite angezeigt.

So aktivieren Sie VeriSign VIP und erzeugen ein VeriSign VIP-Token auf einer Website:

1. Wenn Sie eine Website mit VeriSign VIP-Unterstützung besuchen, zeigt Password Manager eine entsprechende Meldung an.

2. Erstellen Sie Anmeldedaten für den Bildschirm. Weitere Informationen finden Sie unter „Hinzufügen von Anmeldedaten“ auf Seite 34.

3. Wählen Sie im Dialogfeld „Anmeldedaten erstellen“ die Option **I want additional account protection with VIP** (Ich möchte zusätzlichen VIP-Schutz für mein Konto) aus.

So registrieren Sie ein VeriSign VIP-Token bei einer Website:

1. Melden Sie sich manuell oder mithilfe der Password Manager Anmeldedaten bei einer VeriSign VIP-fähigen Website an.
2. Klicken Sie auf das VeriSign VIP-Ballonsymbol, um Anmeldedaten für diese Website zu erstellen.
3. Aktivieren Sie im Dialogfeld „Anmeldedaten zu Password Manager hinzufügen" das Kontrollkästchen **I want VIP security on this site** (Ich möchte VIP-Sicherheit auf dieser Website).

   Diese Option wird nur auf Websites angezeigt, die die VeriSign VIP-Funktion unterstützen. Wenn die VIP-Sicherheit von der betreffenden Website unterstützt wird, können Sie zudem festlegen, dass zusätzlich zur üblichen Authentifizierungsmethode auch Ihr VIP-Sicherheitscode eingegeben wird.

Einstellungen

Sie können Einstellungen zur Personalisierung von HP ProtectTools Security Manager vornehmen:

1. **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern** – Das **Password Manager**-Symbol wird immer dann mit einem Pluszeichen angezeigt, wenn der Anmeldebildschirm einer Website oder eines Programms erkannt wird. Dies zeigt an, dass Sie Anmeldedaten für diesen Bildschirm im Kennwortspeicher hinterlegen können. Um diese Funktion zu deaktivieren, deaktivieren Sie im Dialogfeld **Symboleinstellungen** das Kontrollkästchen neben der Option **Zum Hinzufügen von Anmeldedaten für Anmeldebildschirme auffordern**.
2. **Password Manager mit strg+Windows Logo-Taste+h öffnen** – Die Standardtastenkombination zum Öffnen des Menüs **Password Manager Verknüpfungen** lautet strg+Windows Logo-Taste+h. Zum Ändern der Tastenkombination klicken Sie auf diese Option und geben eine neue Tastenkombination ein. Die Kombinationen können sich aus folgenden Elementen zusammensetzen: strg, alt oder Umschalttaste plus eine beliebige Buchstaben- oder Zifferntaste.
3. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Credential Manager

Mit den Security Manager-Anmeldedaten weisen Sie Ihre Identität nach. Der Administrator dieses Computers kann einstellen, anhand welcher Anmeldedaten Sie Ihre Identität bei Ihrem Windows Konto, bei Websites oder Programmen nachweisen können.

Die verfügbaren Anmeldedaten können je nach integrierten oder an den Computer angeschlossenen Sicherheitsgeräten variieren. Zur Anzeige der unterstützten Anmeldedaten, Anforderungen sowie des aktuellen Status klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager**. Folgende Optionen stehen zur Auswahl:

- Kennwort
- SpareKey
- Fingerabdrücke
- Smart Card
- Gesicht

Um Anmeldedaten festzulegen oder zu ändern, klicken Sie auf den Link, und folgen Sie den Anleitungen auf dem Bildschirm.

Ändern Ihres Windows Kennworts

Mit Security Manager lässt sich Ihr Windows Kennwort schneller und einfacher ändern als über die Systemsteuerung.

Gehen Sie folgendermaßen vor, um Ihr Windows Kennwort zu ändern:

1. Klicken Sie im Security Manager Dashboard auf **Credential Manager** und anschließend auf **Kennwort**.
2. Geben Sie in das Textfeld **Aktuelles Windows Kennwort** Ihr aktuelles Kennwort ein.
3. Geben Sie in das Textfeld **Neues Windows Kennwort** ein neues Kennwort ein, und wiederholen Sie dieses im Textfeld **Neues Kennwort bestätigen**.
4. Klicken Sie auf **Ändern**, um Ihr aktuelles Kennwort sofort durch das soeben eingegebene Kennwort zu ersetzen.

Einrichten eines SpareKey

Die SpareKey-Funktion ermöglicht Ihnen (auf unterstützten Plattformen) den Zugriff auf Ihren Computer, indem Sie drei Sicherheitsfragen aus einer Liste beantworten, die zuvor vom Administrator definiert wurden.

Bei der Ersteinrichtung mithilfe des Einführungsassistenten werden Sie von HP ProtectTools zur Einrichtung Ihres persönlichen SpareKey aufgefordert.

So richten Sie einen persönlichen SpareKey ein:

1. Wählen Sie auf der SpareKey-Seite des Assistenten drei Sicherheitsfragen aus, und beantworten Sie sie.
2. Klicken Sie auf **Weiter**.

Auf der SpareKey-Seite von **Credential Manager** können Sie andere Fragen auswählen bzw. Ihre Antworten ändern.

Nach der Einrichtung können Sie mit dem SpareKey von einem Systemstart-Anmeldebildschirm oder dem Windows Startbildschirm aus auf Ihren Computer zugreifen.

Registrieren Ihrer Fingerabdrücke

Wenn Ihr Computer über ein integriertes oder angeschlossenes Fingerabdruck-Lesegerät verfügt, leitet Sie der Einführungsassistent von HP ProtectTools Security Manager bei der Ersteinrichtung durch die Konfiguration oder „Registrierung” Ihrer Fingerabdrücke. Sie können Ihre Fingerabdrücke

auch auf der Seite „Fingerabdruck" im Security Manager Dashboard unter **Credential Manager** registrieren.

1. Es wird eine Abbildung von zwei Händen angezeigt. Finger, die bereits registriert wurden, werden grün dargestellt. Klicken Sie auf einen Finger in der Darstellung.

   HINWEIS: Wenn Sie einen bereits registrierten Fingerabdruck löschen möchten, klicken Sie auf den entsprechenden Finger.

2. Wenn Sie einen Finger für die Registrierung ausgewählt haben, werden Sie aufgefordert, mit diesem Finger über den Sensor zu streichen, bis der Fingerabdruck erfolgreich registriert wurde. Ein registrierter Finger wird in der Abbildung grün dargestellt.

3. Sie müssen mindestens zwei Finger registrieren, wobei Zeige- und Mittelfinger vorzuziehen sind. Wiederholen Sie die Schritte 1 und 2 für einen weiteren Finger.

4. Klicken Sie auf **Weiter**, und folgen Sie den Anleitungen auf dem Bildschirm.

ACHTUNG: Bei der Registrierung der Fingerabdrücke in der Einführungsphase werden die Fingerabdruckdaten erst mit einem Klick auf **Weiter** gespeichert. Wenn der Computer eine Zeit lang inaktiv ist oder das Programm geschlossen wird, werden die von Ihnen vorgenommenen Änderungen **nicht** gespeichert.

Einrichten einer Smart Card

Administratoren müssen die Smart Card initialisieren und registrieren, bevor sie für die Authentifizierung verwendet werden kann.

Initialisieren der Smart Card

HP ProtectTools Security Manager kann eine Reihe verschiedener Smart Cards unterstützen. Die Anzahl und Art der Zeichen, die für die PIN verwendet werden, können variieren. Der Hersteller der Smart Card stellt normalerweise Tools für die Installation eines Sicherheitszertifikats und einer Verwaltungs-PIN bereit, die HP ProtectTools in seinem Sicherheitsalgorithmus verwendet.

HINWEIS: Die Software ActivIdentity muss installiert werden.

1. Legen Sie die Karte in das Lesegerät ein.

2. Klicken Sie auf **Start**, **Alle Programme** und dann auf **ActivClient PIN Initialization Tool**.

3. Geben Sie eine PIN ein, und bestätigen Sie diese.

4. Klicken Sie auf **Weiter**.

   Die Smart Card-Software stellt Ihnen einen Entsperrschlüssel zur Verfügung. Die meisten Smart Cards sperren sich selbst, wenn die PIN fünfmal falsch eingegeben wird. Der Schlüssel wird zum Entsperren der Karte verwendet.

5. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.

6. Klicken Sie auf **Anmeldeinformationen** und dann auf **Smart Card**.

7. Klicken Sie auf die Registerkarte **Verwaltung**.

8. Vergewissern Sie sich, dass **Smart Card einrichten** ausgewählt ist.

9. Geben Sie Ihre PIN ein, klicken Sie auf **Übernehmen**, und folgen Sie dann den Anleitungen auf dem Bildschirm.
10. Nachdem die Smart Card erfolgreich initialisiert wurde, muss sie noch registriert werden.

Registrieren der Smart Card

Nach der Initialisierung der Smart Card können Administratoren die Karte als Authentifizierungsmethode in HP ProtectTools Administrator-Konsole registrieren:

1. Klicken Sie unter **Zentrale Verwaltung** auf **Installations-Assistent**.
2. Klicken Sie auf der Willkommensseite auf **Weiter**, und geben Sie dann Ihr Windows Kennwort ein.
3. Klicken Sie auf der SpareKey-Seite auf **Skip SpareKey Setup** (SpareKey-Einrichtung überspringen), außer Sie möchten die SpareKey-Informationen aktualisieren.
4. Klicken Sie auf der Seite zum Aktvieren der Sicherheitsfunktionen auf **Weiter**.
5. Vergewissern Sie sich, dass auf der Seite zur Auswahl der Anmeldeinformationen die Option **Smart Card einrichten** ausgewählt ist, und klicken Sie dann auf **Weiter**.
6. Geben Sie auf der Smart Card-Seite Ihre PIN ein, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Benutzer können eine Smart Card in Security Manager registrieren. Weitere Informationen finden Sie in der Hilfe zu Software Security Manager for HP ProtectTools.

Konfigurieren der Smart Card

Wenn der Computer über ein integriertes oder angeschlossenes Lesegerät für Smart Cards verfügt, werden auf der Seite „Smart Card“ folgende Registerkarten angezeigt:

- **Einstellungen** – Sie können den Computer so einstellen, dass er beim Entfernen einer Smart Card automatisch gesperrt wird.

  HINWEIS: Der Computer wird jedoch nur dann gesperrt, wenn die Smart Card als Anmeldeinformation zur Authentifizierung bei der Windows Anmeldung genutzt wurde. Wenn eine Smart Card entfernt wird, die nicht für die Windows Anmeldung verwendet wurde, wird der Computer nicht gesperrt.

- **Verwaltung** – Wählen Sie eine der folgenden Optionen:
  - **Initialize the smart card** (Smart Card initialisieren) – Bereitet eine Smart Card für die Verwendung mit HP Protect Tools vor. Wenn eine Smart Card zuvor bereits außerhalb von HP ProtectTools initialisiert wurde (und ein asymmetrisches Schlüsselpaar sowie das zugehörige Zertifikat enthält), muss sie nicht erneut initialisiert werden, es sei denn, es wird eine Initialisierung mit einem bestimmten Zertifikat gewünscht.
  - **Change smart card PIN** (Smart Card-PIN ändern) – Hiermit können Sie die mit der Smart Card verwendete PIN ändern.

- ◦ **Erase HP ProtectTools data only** (Nur HP ProtectTools Daten löschen) – Löscht nur das während der Karteninitialisierung erstellte HP ProtectTools Zertifikat. Es werden keine anderen Daten von der Karte gelöscht.
- ◦ **Erase all data on the smart card** (Alle Daten von der Smart Card löschen) – Löscht alle Daten von der angegebenen Smart Card. Die Karte kann dann nicht mehr mit HP ProtectTools oder anderen Anwendungen verwendet werden.

HINWEIS: Funktionen, die von Ihrer Smart Card nicht unterstützt werden, sind nicht verfügbar.

▲ Klicken Sie auf **Übernehmen**.

Registrieren von Gesichtsszenen für die Gesichtserkennung

Wenn Ihr Computer über eine integrierte oder angeschlossene Webcam verfügt, leitet Sie der Einführungsassistent von HP ProtectTools Security Manager bei der Ersteinrichtung durch die Konfiguration oder „Registrierung" Ihrer Gesichtsszenen. Sie können Ihre Gesichtsszenen auch auf der Seite für die Gesichtserkennung im Security Manager Dashboard unter **Credential Manager** registrieren.

Um die Anmeldung per Gesichtserkennung nutzen zu können, müssen Sie mindestens eine Gesichtsszene registrieren. Nachdem Sie sich erfolgreich registriert haben, können Sie auch eine neue Szene registrieren, falls während der Anmeldung Probleme auftreten, die mit Änderungen der folgenden Bedingungen zusammenhängen:

- Ihr Gesicht hat sich im Vergleich zur letzten Registrierung erheblich verändert.
- Die Beleuchtung unterscheidet sich wesentlich von der Beleuchtung vorheriger Registrierungen.
- Sie haben bei der letzten Registrierung eine (oder keine) Brille getragen.

HINWEIS: Wenn Sie Schwierigkeiten beim Registrieren von Szenen haben, versuchen Sie, Ihren Abstand zur Webcam zu verringern.

So registrieren Sie eine Gesichtsszene mit dem Einführungsassistenten:

1. Klicken Sie auf der Seite „Gesicht" des Assistenten auf **Erweitert**, und konfigurieren Sie zusätzliche Sicherheitsoptionen. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen" auf Seite 46.
2. Klicken Sie auf **OK**.
3. Klicken Sie auf **Start** oder – falls Sie bereits Gesichtsszenen registriert haben – auf **Neue Szene registrieren**.
4. Wenn Sie keine zusätzlichen Sicherheitsoptionen auswählen, werden Sie zur Auswahl einer zusätzlichen Sicherheitsoption aufgefordert. Folgen Sie den Anleitungen auf dem Bildschirm, und klicken Sie dann auf **Weiter**. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen" auf Seite 46.
5. Klicken Sie auf das **Kamera**-Symbol, und folgen Sie den Anleitungen auf dem Bildschirm, um eine Gesichtsszene zu registrieren.

   Folgen Sie den Anleitungen auf dem Bildschirm, und schauen Sie auf Ihr Bild, während die Szenen aufgezeichnet werden.

6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertig stellen**.

Sie können Gesichtsszenen auch im Security Manager Dashboard registrieren:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 29.
2. Klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf **Erweitert**, und konfigurieren Sie zusätzliche Sicherheitsoptionen. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen“ auf Seite 46.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Start** oder – falls Sie bereits Gesichtsszenen registriert haben – auf **Neue Szene registrieren**.
6. Wenn Sie keine zusätzlichen Sicherheitsoptionen auswählen, werden Sie zur Auswahl einer zusätzlichen Sicherheitsoption aufgefordert. Folgen Sie den Anleitungen auf dem Bildschirm, und klicken Sie dann auf **Weiter**. Weitere Informationen finden Sie unter „Erweiterte Benutzereinstellungen“ auf Seite 46.
7. Klicken Sie auf das **Kamera**-Symbol, und folgen Sie den Anleitungen auf dem Bildschirm, um eine Gesichtsszene zu registrieren.

   Folgen Sie den Anleitungen auf dem Bildschirm, und schauen Sie auf Ihr Bild, während die Szenen aufgezeichnet werden.

Weitere Informationen erhalten Sie in der Hilfe zur Face Recognition Software, indem Sie auf das blaue **?** rechts oben auf der Seite für die Gesichtserkennung klicken.

Erweiterte Benutzereinstellungen

Diese Optionen werden auch auf der Seite „Zusätzliche Sicherheit“ angezeigt, wenn keine weiteren Sicherheitsoptionen ausgewählt wurden.

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 29.
2. Klicken Sie unter **Meine Anmeldedaten** auf **Credential Manager** und dann auf **Gesicht**.
3. Klicken Sie auf **Erweitert**, um die folgenden Sicherheitsoptionen zu konfigurieren:
    a. Registerkarte **Sicherheit** – Wählen Sie eine der folgenden Optionen aus:
        - **No additional security** (Keine zusätzliche Sicherheitsoption) – Wählen Sie diese Option aus, falls Sie keine zusätzliche Sicherheitsoption für die Gesichtserkennung definieren möchten.
        - **Use PIN for additional security** (PIN für zusätzliche Sicherheit verwenden) – Wählen Sie diese Option aus, falls eine benutzerspezifische PIN für die Gesichtserkennung erforderlich sein soll.
            - Klicken Sie auf **PIN erstellen**.
            - Geben Sie Ihr Windows Kennwort ein.
            - Geben Sie die neue PIN ein, und bestätigen Sie sie, indem Sie die Eingabe wiederholen.

              Nach der PIN-Erstellung stehen die folgenden Optionen zur Auswahl: **Ändern**, **Zurücksetzen** und **PIN entfernen**.
        - **Use PIN for additional security** (PIN für zusätzliche Sicherheit verwenden) – Wählen Sie diese Option, falls Ihr Bluetooth-fähiges Telefon mit der Gesichtserkennung gekoppelt werden soll. Nachdem bei der Windows Anmeldung Ihr Gesicht erkannt wurde, überprüft Face Recognition, ob das gekoppelte Bluetooth Telefon vorhanden ist. Wenn es vorhanden (und Bluetooth aktiviert) ist, können Sie sich bei Windows anmelden.
            - Vergewissern Sie sich, dass Bluetooth sowohl am Computer als auch am Telefon aktiviert ist.

              Wenn kein Telefon mit aktivierter Bluetooth Funktion vorhanden ist, werden Sie aufgefordert, das gekoppelte Bluetooth Telefon zu aktivieren und den Anmeldevorgang zu wiederholen. Nach 30 Sekunden wird die Anzeige des Face Recognition Anmeldefensters beendet. Zum Starten des Anmeldevorgangs klicken Sie auf das **Kamera**-Symbol. Wenn kein Telefon mit aktivierter Bluetooth Funktion vorhanden ist, können Sie sich auch mit Ihrem normalen Windows Kennwort anmelden.
            - Klicken Sie auf **Hinzufügen**.
            - Wenn Ihr Bluetooth Gerät angezeigt wird, wählen Sie es aus und klicken dann auf **Weiter**.

        Klicken Sie auf **OK**.

    b. Registerkarte **Sonstige Einstellungen** – Aktivieren Sie die Kontrollkästchen, um eine oder mehrere der folgenden Optionen auszuwählen. Wenn Sie eine Funktion nicht auswählen

möchten, deaktivieren Sie das betreffende Kontrollkästchen. Die hier vorgenommenen Einstellungen gelten nur für den aktuellen Benutzer.

- **Klang bei Gesichtserkennungsereignissen abspielen** – Wenn die Gesichtserkennung erfolgreich ist bzw. fehlschlägt, wird ein akustisches Signal ausgegeben.
- **Bei fehlgeschlagener Anmeldung zum Aktualisieren von Szenen auffordern** – Wenn die Gesichtserkennung fehlgeschlagen ist, Sie Ihr Kennwort jedoch erfolgreich eingegeben haben, werden Sie unter Umständen zum Speichern mehrerer Gesichtsszenen aufgefordert, um die Chancen einer erfolgreichen Gesichtserkennung in der Zukunft zu erhöhen.
- **Bei fehlgeschlagener Anmeldung zum Registrieren einer neuen Szene auffordern** – Wenn die Gesichtserkennung zwar fehlgeschlagen ist, Sie Ihr Kennwort jedoch erfolgreich eingegeben haben, werden Sie unter Umständen zur Registrierung einer neuen Szene aufgefordert, um die Chancen einer erfolgreichen Gesichtserkennung in der Zukunft zu erhöhen.

Klicken Sie auf **OK**.

Ihre persönliche ID-Card

Ihre ID-Card identifiziert Sie eindeutig als Eigentümer dieses Windows Kontos und zeigt Ihren Namen und ein Bild Ihrer Wahl an. Sie wird deutlich oben links auf den Seiten von Security Manager angezeigt.

Sie können das Bild und die Art der Anzeige Ihres Namens ändern. Standardmäßig werden Ihr vollständiger Windows Benutzername und das Bild angezeigt, das Sie bei der Windows Einrichtung ausgewählt haben.

So ändern Sie den angezeigten Namen:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 29.
2. Klicken Sie auf die ID-Card links oben im Dashboard.
3. Klicken Sie auf das Feld mit Ihrem Windows Benutzernamen für dieses Konto, geben Sie einen neuen Namen ein, und klicken Sie dann auf **Speichern**.

So ändern Sie das angezeigte Bild:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 29.
2. Klicken Sie auf die ID-Card links oben im Dashboard.
3. Klicken Sie auf **Bild wählen**; klicken Sie dann auf ein Bild und anschließend auf **Speichern**.

Festlegen der Einstellungen

Sie können die Einstellungen für HP ProtectTools Security Manager personalisieren. Klicken Sie im Security Manager-Dashboard auf **Erweitert** und anschließend auf **Voreinstellungen**. Die verfügbaren Einstellungen werden auf zwei Registerkarten angezeigt: **Allgemein** und **Fingerabdruck**.

Registerkarte „Allgemein“

Darstellung – **Show icon in taskbar notification area** (Symbol im Infobereich der Taskleiste anzeigen)

- Um die Anzeige des Symbols in der Taskleiste zu aktivieren, aktivieren Sie dieses Kontrollkästchen.
- Um die Anzeige des Symbols in der Taskleiste zu deaktivieren, deaktivieren Sie dieses Kontrollkästchen.

Registerkarte „Fingerabdruck“

HINWEIS: Die Registerkarte **Fingerabdruck** ist nur verfügbar, wenn der Computer über ein Fingerabdruck-Lesegerät verfügt und der korrekte Treiber installiert ist.

- **Schnellaktionen** – Hiermit können Sie die Security Manager Aufgaben auswählen, die ausgeführt werden sollen, wenn Sie eine bestimmte Taste gedrückt halten, während Sie mit dem Finger über den Sensor streichen.

  Um eine Schnellaktion zu einer der aufgelisteten Tastenkombinationen hinzuzufügen, klicken Sie auf eine der Optionen **(Taste) + Fingerabdruck**, und wählen Sie eine der verfügbaren Aufgaben aus dem Menü aus.

- **Fingerabdruckscan-Feedback** – Wird nur angezeigt, wenn ein Fingerabdruck-Lesegerät verfügbar ist. Verwenden Sie diese Einstellung, um das Feedback anzupassen, das Sie erhalten, wenn Sie mit dem Finger über den Sensor streichen.

  - **Sound-Feedback aktivieren** – Security Manager gibt akustische Signale aus, wenn ein Fingerabdruck durch Streichen über den Sensor registriert wurde, wobei für spezifische Programmereignisse verschiedene Signale verwendet werden. Sie können diesen Ereignissen auf der Registerkarte **Sounds** in der Windows Systemsteuerung andere Töne zuweisen oder akustische Signale ausschalten, indem Sie diese Option deaktivieren.

  - **Feedback zur Scanqualität anzeigen**

    Um alle durch Streichen über den Sensor registrierten Fingerabdrücke unabhängig von der Qualität anzuzeigen, aktivieren Sie das Kontrollkästchen.

    Um nur Fingerabdrücke guter Qualität anzuzeigen, deaktivieren Sie das Kontrollkästchen.

Sichern und Wiederherstellen Ihrer Daten

Es wird empfohlen, regelmäßig eine Sicherungskopie der Security Manager-Daten zu erstellen. Wie oft dies erforderlich ist, hängt davon ab, wie häufig sich die Daten ändern. Wenn Sie beispielsweise täglich neue Anmeldedaten hinzufügen, sollten Sie Ihre Daten auch täglich sichern.

Sicherungskopien können auch für die Migration von einem Computer auf einen anderen verwendet werden (importieren und exportieren).

HINWEIS: Mit dieser Funktion werden nur die Daten gesichert.

HP ProtectTools Security Manager muss auf jedem Computer installiert werden, auf dem gesicherte Daten gespeichert werden sollen, andernfalls können die Daten aus der Sicherungskopie nicht wiederhergestellt werden.

So sichern Sie Ihre Daten:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager“ auf Seite 29.
2. Klicken Sie links im Dashboard auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten sichern**.
4. Wählen Sie die Module aus, die gesichert werden sollen. In den meisten Fällen empfiehlt es sich, alle Module auszuwählen.
5. Identität bestätigen.

6. Geben Sie einen Namen für die Speicherdatei ein. Die Datei wird standardmäßig im Ordner „Dokumente" gespeichert. Klicken Sie auf **Durchsuchen**, um einen anderen Speicherort anzugeben.
7. Geben Sie ein Kennwort ein, um die Datei zu schützen.
8. Klicken Sie auf **Fertig stellen**.

So stellen Sie Ihre Daten wieder her:

1. Öffnen Sie das Security Manager Dashboard. Weitere Informationen finden Sie unter „Öffnen von Security Manager" auf Seite 29.
2. Klicken Sie links im Dashboard auf **Erweitert** und anschließend auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Daten wiederherstellen**.
4. Wählen Sie die zuvor erstellte Speicherdatei aus. Geben Sie den Pfad in das entsprechende Feld ein, oder klicken Sie auf **Durchsuchen**.
5. Geben Sie das zuvor verwendete Kennwort zum Schützen der Datei ein.
6. Wählen Sie die Module aus, deren Daten wiederhergestellt werden sollen. In den meisten Fällen empfiehlt es sich, alle aufgeführten Module auszuwählen.
7. Bestätigen Sie Ihr Windows Kennwort.
8. Klicken Sie auf **Fertig stellen**.

5 Drive Encryption for HP ProtectTools (nur ausgewählte Modelle)

Drive Encryption for HP ProtectTools bietet eine umfassende Datenschutzlösung durch Verschlüsselung der Festplatte Ihres Computers. Wenn Drive Encryption aktiviert ist, müssen Sie sich auf dem Drive Encryption-Anmeldebildschirm anmelden, der vor dem Starten des Windows® Betriebssystems angezeigt wird.

Mit dem Installations-Assistenten für HP ProtectTools Security Manager können Windows Administratoren Drive Encryption aktivieren, den Verschlüsselungsschlüssel sichern und Laufwerke auswählen oder deaktivieren. Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager-Software.

Die folgenden Aufgaben können mit Drive Encryption durchgeführt werden:

- Auswahl der Drive Encryption-Einstellungen:
  - Aktivieren eines TPM-geschützten Kennworts
  - Ver- und Entschlüsseln einzelner Laufwerke oder Partitionen mit Software-Verschlüsselung
  - Ver- und Entschlüsseln einzelner selbstverschlüsselnder Laufwerke mit Hardware-Verschlüsselung
  - Erhöhen der Sicherheit durch Deaktivierung von Standby und Energiesparmodus um sicherzustellen, dass die Systemstart-Authentifizierung von Drive Encryption immer erforderlich ist

  HINWEIS: Nur interne SATA- und externe eSATA-Festplatten können verschlüsselt werden.

- Erstellen von Sicherungsschlüsseln
- Wiederherstellen eines Drive Encryption-Schlüssels
- Aktivieren der Systemstart-Authentifizierung von Drive Encryption per Kennwort, registriertem Fingerabdruck oder Smart Card-PIN

Öffnen von Drive Encryption

Administratoren können auf Drive Encryption über HP ProtectTools Administrator-Konsole zugreifen.

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Drive Encryption**.

Allgemeine Aufgaben

Aktivieren von Drive Encryption für Standard-Festplatten

Standard-Festplatten werden mit Softwareverschlüsselung verschlüsselt. Um Drive Encryption zu aktivieren, führen Sie die folgenden Schritte aus:

1. Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
2. Folgen Sie den Anleitungen auf dem Bildschirm, bis die Seite **Sicherheitsfunktionen aktivieren** angezeigt wird, und fahren Sie anschließend mit Schritt 4 unten fort.

– oder –

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

   HINWEIS: Wenn keine Festplatte zur Verschlüsselung ausgewählt ist, wird die Systemstart-Authentifizierung von Drive Encryption aktiviert, aber die Festplatte(n) wird/werden nicht verschlüsselt.

5. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**
6. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den richtigen Steckplatz an.

   HINWEIS: Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden. Zur Sicherung kann eine Diskette, ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MMC verwendet werden.

7. Aktivieren Sie unter **Drive Encryption-Schlüssel sichern** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
8. Klicken Sie auf **Weiter**.

   HINWEIS: Der Computer wird neu gestartet.

Drive Encryption wurde aktiviert. Die Verschlüsselung der Festplatte kann, je nach Größe des Laufwerks, einige Stunden dauern.

Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager-Software.

Aktivieren von Drive Encryption für selbstverschlüsselnde Festplatten

Selbstverschlüsselnde Laufwerke nach den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung selbstverschlüsselnder Laufwerke lassen sich entweder mit Software- oder mit

Hardwareverschlüsselung verschlüsseln. Gehen Sie wie folgt vor, um Drive Encryption für selbstverschlüsselnde Laufwerke zu aktivieren:

1. Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
2. Folgen Sie den Anleitungen auf dem Bildschirm, bis die Seite **Sicherheitsfunktionen aktivieren** angezeigt wird, und fahren Sie anschließend mit Schritt 4 entweder unter „Softwareverschlüsselung“ oder unter „Hardwareverschlüsselung“ fort.

HINWEIS: Wenn Ihr Computer nicht über ein selbstverschlüsselndes Laufwerk verfügt, das den OPAL-Spezifikationen der Trusted Computing Group für die Verwaltung selbstverschlüsselnder Laufwerke entspricht, ist die Option Hardwareverschlüsselung nicht verfügbar, und es wird die Softwareverschlüsselung verwendet.

Bei einer Mischung selbstverschlüsselnder und Standard-Laufwerke ist die Option Hardwareverschlüsselung nicht verfügbar, und es wird die Softwareverschlüsselung verwendet.

– oder –

Softwareverschlüsselung

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.
5. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**
6. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den richtigen Steckplatz an.

   HINWEIS: Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden. Zur Sicherung kann eine Diskette, ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MMC verwendet werden.
7. Aktivieren Sie unter **Drive Encryption-Schlüssel sichern** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
8. Klicken Sie auf **Übernehmen**.

   HINWEIS: Der Computer wird neu gestartet.

   Drive Encryption wurde aktiviert. Die Verschlüsselung der Festplatte kann, je nach Größe des Laufwerks, einige Stunden dauern.

Hardwareverschlüsselung

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Aktivieren Sie das Kontrollkästchen **Drive Encryption**, und klicken Sie dann auf **Weiter**.

   HINWEIS: Wenn nur ein Laufwerk angezeigt wird, wird das Kontrollkästchen für das Laufwerk automatisch ausgewählt und abgeblendet.

   Wenn mehr als ein Laufwerk angezeigt wird, werden die Kontrollkästchen automatisch ausgewählt, aber nicht abgeblendet.

   Die Schaltfläche **Weiter** ist nur dann verfügbar, wenn mindestens ein Laufwerk ausgewählt ist.

5. Vergewissern Sie sich, dass das Kontrollkästchen **Hardwareverschlüsselung für Laufwerk verwenden** unten im Bildschirm markiert ist.
6. Aktivieren Sie unter **Zu verschlüsselnde Laufwerke** das Kontrollkästchen für die Festplatte, die verschlüsselt werden soll, und klicken Sie dann auf **Weiter**
7. Um den Verschlüsselungsschlüssel zu sichern, schließen Sie das Speichergerät an den richtigen Steckplatz an.

   HINWEIS: Um den Verschlüsselungsschlüssel zu speichern, müssen Sie ein USB-Speichergerät im FAT32-Format verwenden. Zur Sicherung kann eine Diskette, ein USB Memory Stick, eine Secure Digital (SD) Memory Card oder eine MMC verwendet werden.

8. Aktivieren Sie unter **Drive Encryption-Schlüssel sichern** das Kontrollkästchen für das Speichergerät, auf dem der Verschlüsselungsschlüssel gespeichert werden soll.
9. Klicken Sie auf **Übernehmen**.

   HINWEIS: Der Computer muss neu gestartet werden.

   Drive Encryption wurde aktiviert. Die Verschlüsselung des Laufwerks kann einige Minuten dauern.

Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager-Software.

Deaktivieren von Drive Encryption

Administratoren können den Installations-Assistenten von HP ProtectTools Security Manager verwenden, um Drive Encryption zu deaktivieren. Weitere Informationen finden Sie in der Hilfe zur HP ProtectTools Security Manager-Software.

▲ Folgen Sie den Anleitungen auf dem Bildschirm, bis die Seite **Sicherheitsfunktionen aktivieren** angezeigt wird, und fahren Sie anschließend mit Schritt 4 unten fort.

– ODER –

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Sicherheit**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Funktionen**.
4. Entfernen Sie die Markierung des Kontrollkästchens **Drive Encryption**, und klicken Sie dann auf **Weiter**.

   Die Deaktivierung der Verschlüsselung wird gestartet.

   HINWEIS: Wenn Softwareverschlüsselung verwendet wurde, wird die Entschlüsselung gestartet. Dies kann, je nach Größe des Laufwerks, einige Stunden dauern. Sobald die Entschlüsselung abgeschlossen ist, wird Drive Encryption deaktiviert.

   Wenn Hardwareverschlüsselung verwendet wurde, wird das Laufwerk sofort entschlüsselt. Dies kann ein paar Minuten dauern. Anschließend wird Drive Encryption deaktiviert.

   Sobald das Laufwerk deaktiviert ist, muss der Computer neu gestartet werden.

Anmelden, nachdem Drive Encryption aktiviert wurde

Wenn Sie den Computer einschalten, nachdem Drive Encryption aktiviert und Ihr Benutzerkonto registriert wurde, müssen Sie sich beim Drive Encryption-Anmeldebildschirm anmelden:

HINWEIS: Stellen Sie bei Hardwareverschlüsselung sicher, dass der Computer ausgeschaltet wird. Wenn der Computer nicht ausgeschaltet und dann neu gestartet wird, wird der Bildschirm für die Systemstart-Authentifizierung von Drive Encryption nicht angezeigt.

HINWEIS: Bei einem Start aus dem Standby- oder dem Energiesparmodus wird die Systemstart-Authentifizierung von Drive Encryption für Software- und Hardwareverschlüsselung nicht angezeigt, es sei denn, diese sind deaktiviert.

Bei einem Start aus dem Ruhezustand wird die Systemstart-Authentifizierung von Drive Encryption angezeigt.

HINWEIS: Wenn der Windows Administrator die Systemstartsicherheit in HP ProtectTools Security Manager aktiviert hat, können Sie sich sofort nach dem Einschalten am Computer anmelden, statt erst im Anmeldebildschirm von Drive Encryption.

1. Klicken Sie auf Ihren Benutzernamen, und geben Sie anschließend Ihr Windows Kennwort oder Ihre Smart Card-PIN ein, oder streichen Sie mit einem registrierten Finger über den Sensor.

   HINWEIS: Folgende Smart Cards werden unterstützt:



Smart Cards

- ActivIdentity 64K V2C Smart Card
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

PCMCIA-Lesegeräte

- Express Card 54 SCR3340, internes Lesegerät
- SCR 201
- SCR 243 (auch von HP)
- ActivCard
- Omnikey 4040
- Cisco

USB-Lesegeräte

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP Smart Card-Terminal

2. Klicken Sie auf **OK**.

HINWEIS: Wenn Sie einen Wiederherstellungsschlüssel zur Anmeldung beim Anmeldebildschirm von Drive Encryption verwenden, müssen Sie sich mit Ihrem Kennwort, Ihrer Smart Card-PIN oder einem registrierten Fingerabdruck beim Windows Anmeldebildschirm anmelden.

Schützen Ihrer Daten durch Verschlüsselung der Festplatte

Es wird empfohlen, den Installations-Assistenten von HP ProtectTools Security Manager zu verwenden, um Daten durch Verschlüsselung der Festplatte zu schützen:

1. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Drive Encryption**, um die verfügbaren Optionen aufzurufen.
2. Klicken Sie auf **Einstellungen**.
3. Bei Laufwerken mit Softwareverschlüsselung wählen Sie die Laufwerkspartitionen für die Verschlüsselung aus.

   HINWEIS: Dies gilt auch für den Fall, dass eine oder mehrere Standardfestplatten und ein oder mehrere selbstverschlüsselnde Laufwerke vorhanden sind.

– oder –

▲ Bei Laufwerken mit Hardwareverschlüsselung wählen Sie das/die Laufwerk(e) für die Verschlüsselung aus. Mindestens ein Laufwerk muss ausgewählt werden.

Anzeigen der Verschlüsselungsstatus

Benutzer können den Verschlüsselungsstatus von HP ProtectTools Security Manager aus anzeigen.

HINWEIS: Administratoren können den Drive Encryption-Status mithilfe von HP ProtectTools Administrator-Konsole ändern.

1. Öffnen Sie HP ProtectTools Security Manager.
2. Klicken Sie unter **Meine Daten** auf **Drive Encryption**.

   Bei Softwareverschlüsselung wird einer der folgenden Statuscodes unter **Laufwerkstatus** angezeigt:

   - Aktiviert
   - Deaktiviert
   - Nicht verschlüsselt
   - Verschlüsselt
   - Wird gerade verschlüsselt
   - Wird gerade entschlüsselt

   Bei Hardwareverschlüsselung wird der folgende Statuscode unter **Laufwerkstatus** angezeigt:

   - Verschlüsselt

   Wenn die Festplatte gerade verschlüsselt oder entschlüsselt wird, wird eine Fortschrittsanzeige mit Angabe des Prozentsatzes der Durchführung und der noch verbleibenden Zeit bis zum Abschluss der Verschlüsselung oder Entschlüsselung angezeigt.

Erweiterte Aufgaben

Verwalten von Drive Encryption (Administrator-Aufgabe)

Auf der Einstellungsseite von Drive Encryption können Administratoren den Status von Drive Encryption anzeigen und ändern (Aktiviert, Deaktiviert oder Hardwareverschlüsselung wurde aktiviert) und den Verschlüsselungsstatus aller Festplatten auf dem Computer anzeigen.



HINWEIS: Die Hardwareverschlüsselung kann auf der Einstellungsseite nicht geändert werden.

- Wenn der Status deaktiviert ist, wurde Drive Encryption noch nicht vom Windows Administrator aktiviert, und der Festplattenschutz ist nicht aktiv. Verwenden Sie den Installations-Assistenten von HP ProtectTools Security Manager, um Drive Encryption zu aktivieren.
- Wenn der Status aktiviert ist, wurde Drive Encryption aktiviert und konfiguriert. Das Laufwerk befindet sich in einem der folgenden Status:

Softwareverschlüsselung

- ◦ Nicht verschlüsselt
- ◦ Verschlüsselt
- ◦ Wird gerade verschlüsselt
- ◦ Wird gerade entschlüsselt

Hardwareverschlüsselung

- Verschlüsselt

Ver- und Entschlüsseln einzelner Laufwerke (nur Softwareverschlüsselung)

Administratoren können auf der Einstellungsseite eine oder mehrere Festplatten auf dem Computer verschlüsseln oder ein bereits verschlüsseltes Laufwerk entschlüsseln.

1. Öffnen Sie HP ProtectTools Administrator-Konsole.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Drive Encryption**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Einstellungen**.
4. Aktivieren oder deaktivieren Sie unter **Laufwerkstatus** das Kontrollkästchen für die Festplatte, die verschlüsselt oder entschlüsselt werden soll, und klicken Sie dann auf **Übernehmen**

HINWEIS: Wenn die Festplatte gerade verschlüsselt oder entschlüsselt wird, wird eine Fortschrittsanzeige mit der noch verbleibenden Zeit bis zum Abschluss der aktuellen Sitzung angezeigt.

Wenn der Computer während der Verschlüsselung heruntergefahren wird oder in den Standby- oder Energiesparmodus oder den Ruhezustand wechselt und dann neu gestartet wird, wird die Zeit auf der Fortschrittsanzeige auf den Beginn zurückgesetzt, die Verschlüsselung wird aber dort fortgesetzt, wo sie unterbrochen wurde. Die Fortschrittsanzeige in Prozent und die verbleibende Zeit ändern sich schneller, was auf den vorhergehenden Prozess zurückzuführen ist.

HINWEIS: Dynamische Partitionen werden nicht unterstützt. Wenn eine Partition als verfügbar angezeigt wird, sich aber nicht verschlüsseln lässt, so handelt es sich um eine dynamische Partition. Eine dynamische Partition entsteht, wenn eine vorhandene Partition zum Erstellen einer neuer Partition in der Festplattenverwaltung geschrumpft wird.

Eine Warnmeldung wird angezeigt, wenn eine Partition in eine dynamische Partition umgewandelt wird.

Sicherung und Wiederherstellung (Administrator-Aufgabe)

Wenn Drive Encryption aktiviert ist, können Administratoren die Sicherungsseite für den Verschlüsselungsschlüssel verwenden, um Verschlüsselungsschlüssel auf Wechselmedien zu sichern und eine Wiederherstellung durchzuführen.

Sichern von Verschlüsselungsschlüsseln

Administratoren können den Verschlüsselungsschlüssel für ein verschlüsseltes Laufwerk auf einem Wechselmediengerät sichern.

ACHTUNG: Das Speichergerät mit dem Verschlüsselungsschlüssel muss an einem sicheren Ort aufbewahrt werden, denn wenn Sie das Kennwort vergessen, Ihre Smart Card verlieren oder keinen Fingerabdruck registriert haben, stellt dieses Gerät die einzige Zugriffsmöglichkeit auf die Festplatte dar.

1. Öffnen Sie HP ProtectTools Administrator-Konsole.
2. Klicken Sie im linken Fensterausschnitt auf das Symbol **+** links von **Drive Encryption**, um die verfügbaren Optionen aufzurufen.
3. Klicken Sie auf **Encryption Key Backup** (Sichern des Sicherungsschlüssels).
4. Schließen Sie das Speichergerät an, das zur Sicherung des Verschlüsselungsschlüssels verwendet werden soll.
5. Aktivieren Sie unter **Laufwerk** das Kontrollkästchen für das Gerät, auf dem der Verschlüsselungsschlüssel gesichert werden soll.
6. Klicken Sie auf **Schlüssel sichern**.
7. Lesen Sie den dargestellten Text, und klicken Sie dann auf **Weiter**. Der Verschlüsselungsschlüssel wird auf dem von Ihnen ausgewählten Speichergerät gespeichert.

Wiederherstellen von Verschlüsselungsschlüsseln

Administratoren können einen Verschlüsselungsschlüssel von einem Wechselmediengerät aus wiederherstellen, auf dem er zuvor gesichert wurde:

1. Schalten Sie den Computer ein.
2. Schließen Sie das Wechselmediengerät an, das Ihren Sicherungsschlüssel enthält.
3. Klicken Sie im Anmeldedialogfeld für Drive Encryption for HP ProtectTools auf **Optionen**.
4. Klicken Sie auf **Wiederherstellung**.
5. Wählen Sie die Datei aus, die Ihren Sicherungsschlüssel enthält, oder klicken Sie auf **Durchsuchen**, um die Datei zu suchen, und klicken Sie danach auf **Weiter**.
6. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Ihr Computer wird gestartet.

   HINWEIS: Nach der Wiederherstellung sollten Sie Ihr Kennwort unbedingt zurücksetzen.

6 Privacy Manager for HP ProtectTools (bestimmte Modelle)

Privacy Manager für HP ProtectTools ermöglicht Ihnen die Nutzung von erweiterten Sicherheits-Anmeldemethoden (Authentifizierung), um die Quelle, die Integrität und die Sicherheit bei der Übertragung von E-Mails oder Microsoft® Office-Dokumenten zu überprüfen.

Privacy Manager ergänzt die Sicherheitsinfrastruktur von HP ProtectTools Security Manager, die die folgenden Sicherheits-Anmeldemethoden umfasst:

- Fingerabdruck-Authentifizierung
- Windows® Kennwort
- Smart Card
- Gesichtserkennung

Sie können jede der vorstehend genannten Sicherheits-Anmeldemethoden in Privacy Manager verwenden.

Öffnen von Privacy Manager

So öffnen Sie Privacy Manager:

- Sie erhalten Zugriff auf Outlook-spezifische Funktionen in Microsoft Outlook, indem Sie auf der Registerkarte **Nachricht** in der Gruppe **Datenschutz** auf **Sicher senden** klicken.
- Sie erhalten Zugriff auf die meisten Funktionen in Microsoft Office-Dokumenten, indem Sie auf der Registerkarte **Startseite** in der Gruppe **Datenschutz** auf **Signieren und verschlüsseln** klicken.
- Zugriff auf zusätzliche Funktionen erhalten Sie über das HP ProtectTools Security Manager-Dashboard.
    - Klicken Sie auf **Start**, **Alle Programme**, **HP**, **HP ProtectTools Security Manager** und danach auf **Privacy Manager**.

      – oder –
    - Klicken Sie auf die Desktop-Minianwendung **HP ProtectTools**.

      – oder –
    - Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **Privacy Manager** und anschließend auf **Konfiguration**.

Setup-Verfahren

Verwalten von Privacy Manager Zertifikaten

Privacy Manager-Zertifikate schützen Daten und Nachrichten mithilfe der Verschlüsselungstechnik PKI (Public Key Infrastructure). Für diese Verschlüsselungstechnik benötigen die Benutzer Verschlüsselungsschlüssel und ein Privacy Manager-Zertifikat, das von einer Zertifizierungsstelle (CA) ausgestellt wird. Im Gegensatz zu den meisten Datenverschlüsselungs- und Authentifizierungsprogrammen, die lediglich eine regelmäßige Authentifizierung verlangen, erfordert Privacy Manager für jede Signierung einer E-Mail-Nachricht oder eines Microsoft Office Dokuments eine Authentifizierung mit einem Verschlüsselungsschlüssel. Privacy Manager garantiert das sichere Speichern und Senden wichtiger Informationen.

Mit dem Certificate Manager können Sie folgende Aufgaben ausführen:

- „Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62
- „Abrufen eines vorab zugewiesenen Privacy Manager-Unternehmenszertifikats“ auf Seite 63
- „Festlegen eines Privacy Manager-Standardzertifikats“ auf Seite 66
- „Importieren eines Zertifikats von einem anderen Anbieter“ auf Seite 63
- „Anzeigen der Details eines Privacy Manager-Zertifikats“ auf Seite 64
- „Erneuern eines Privacy Manager-Zertifikats“ auf Seite 64
- „Festlegen eines Privacy Manager-Standardzertifikats“ auf Seite 66
- „Löschen eines Privacy Manager-Zertifikats“ auf Seite 66
- „Wiederherstellen eines Privacy Manager-Zertifikats“ auf Seite 66
- „Widerrufen eines Privacy Manager-Zertifikats“ auf Seite 67

Anfordern eines Privacy Manager-Zertifikats

Um Zugriff auf die Privacy Manager-Funktionen zu erhalten, muss zunächst ein Privacy Manager-Zertifikat (aus Privacy Manager heraus) mit einer gültigen E-Mail-Adresse angefordert und installiert werden. Die E-Mail-Adresse muss als Konto von Microsoft Outlook auf dem Computer eingerichtet sein, von dem aus das Privacy Manager-Zertifikat angefordert wird.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Privacy Manager-Zertifikat anfordern**.
3. Lesen Sie den Text auf dem Anfangsbildschirm, und klicken Sie dann auf **Weiter**.
4. Lesen Sie den Lizenzvertrag auf der Seite „Lizenzvertrag“.
5. Aktivieren Sie das Kontrollkästchen neben **Check here to accept the terms of this license agreement** (Hier klicken, um die Lizenzvereinbarung anzunehmen), und klicken Sie dann auf **Weiter**.
6. Geben Sie auf der Seite „Ihre Zertifikatsdetails“ die erforderlichen Angaben ein, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf der Seite „Zertifikatanforderung akzeptiert“ auf **Fertig stellen**.

Sie erhalten eine E-Mail in Microsoft Outlook, in deren Anhang Sie Ihr Privacy Manager-Zertifikat finden.

Abrufen eines vorab zugewiesenen Privacy Manager-Unternehmenszertifikats

1. Öffnen Sie in Outlook die E-Mail, in der Sie darüber informiert wurden, dass Ihnen ein Unternehmenszertifikat vorab zugewiesen wurde.
2. Klicken Sie auf **Abrufen**.

Sie erhalten eine E-Mail in Microsoft Outlook, in deren Anhang Sie Ihr Privacy Manager-Zertifikat finden.

Informationen zum Installieren des Zertifikats finden Sie unter „Einrichten eines Privacy Manager-Zertifikats“ auf Seite 63.

Einrichten eines Privacy Manager-Zertifikats

1. Wenn Sie die E-Mail mit Ihrem Privacy Manager-Zertifikat erhalten haben, öffnen Sie sie, und klicken Sie auf die Schaltfläche **Setup**. Diese befindet sich in Outlook 2007 bzw. Outlook 2010 unten rechts und in Outlook 2003 oben links in der Nachricht.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
3. Klicken Sie auf der Seite „Zertifikat installiert“ auf **Weiter**.
4. Geben Sie auf der Seite „Zertifikatsicherung“ einen Speicherort und einen Namen für die Sicherungsdatei ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen.

   ⚠ **ACHTUNG:** Speichern Sie die Datei nicht auf der Festplatte, und bewahren Sie das Speichermedium an einem sicheren Platz auf. Diese Datei ist ausschließlich zu Ihrer Verwendung bestimmt und wird benötigt, wenn Sie Ihr Privacy Manager-Zertifikat und die zugehörigen Schlüssel wiederherstellen müssen.

5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.
6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Wenn Sie den Einladungsvorgang für vertrauenswürdige Kontakte starten möchten, folgen Sie den Anleitungen auf dem Bildschirm beginnend mit Schritt 2 unter „Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte“ auf Seite 68.

   – oder –

   Wenn Sie auf **Abbrechen** klicken, finden Sie unter „Verwalten vertrauenswürdiger Kontakte“ auf Seite 67 Informationen darüber, wie Sie zu einem späteren Zeitpunkt einen vertrauenswürdigen Kontakt hinzufügen können.

Importieren eines Zertifikats von einem anderen Anbieter

Sie können das Zertifikat eines anderen Anbieters möglicherweise mithilfe des Assistenten zum Importieren eines Zertifikats in Privacy Manager importieren.

Damit Sie diese Funktion nutzen können, muss auf der Seite „Einstellungen“ unter **Privacy Manager** in HP ProtectTools Administrator-Konsole die Einstellung **Verwendung von Zertifikaten anderer Anbieter zulassen** aktiviert sein.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Wählen Sie die Registerkarte **Certificate Manager** aus, und klicken Sie dann auf **Zertifikate importieren**.

   Diese Schaltfläche wird nicht angezeigt, wenn das Importieren von Zertifikaten nicht zulässig ist.
3. Wählen Sie ein bereits auf dem Computer installiertes Zertifikat oder eine PFX-Datei (Datei für den privaten Informationsaustausch/PKCS#12) für den Import aus, und klicken Sie danach auf **Weiter**.
   - Um ein bereits auf dem Computer installiertes Zertifikat zu importieren, wählen Sie das gewünschte Zertifikat aus, und klicken Sie danach auf **Weiter**.
   - Zum Auswählen eines PFX-Zertifikats klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort der PFX-Datei, und klicken Sie dann auf **Weiter**. Geben Sie das Passwort für die PFX-Datei ein, und klicken Sie anschließend auf **Weiter**.
4. Nach Abschluss des Importvorgangs klicken Sie auf **Weiter**.
5. Sie haben die Möglichkeit, das importierte Zertifikat zu sichern.

   Es wird empfohlen, das Zertifikat an einem anderen Speicherort als auf der Festplatte Ihres Computers zu sichern.

Anzeigen der Details eines Privacy Manager-Zertifikats

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf ein Privacy Manager-Zertifikat.
3. Klicken Sie auf **Zertifikatdetails**.
4. Wenn Sie die Details gelesen haben, klicken Sie auf **OK**.

Erneuern eines Privacy Manager-Zertifikats

Sie werden vor Ablauf Ihres Privacy Manager-Zertifikats daran erinnert, dass Sie das Zertifikat erneuern müssen:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Zertifikat erneuern**.
3. Folgen Sie den Anleitungen auf dem Bildschirm, um ein neues Privacy Manager-Zertifikat zu erhalten.

HINWEIS: Durch die Erneuerung Ihres Privacy Manager-Zertifikats wird Ihr altes Privacy Manager-Zertifikat nicht ersetzt. Sie müssen ein neues Privacy Manager-Zertifikat anfordern und dann die gleichen Schritte wie unter „Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62 beschrieben ausführen.

Bei Unternehmenszertifikaten, die von Ihrem Unternehmen mithilfe von Microsoft Certificate Authority ausgestellt wurden, muss der CA-Administrator Ihr Zertifikat mit demselben privaten Schlüssel erneuern, der auch für das ursprüngliche Zertifikat verwendet wurde. Er kann aber auch ein neues Zertifikat unter Verwendung desselben privaten Schlüssels ausstellen.

Festlegen eines Privacy Manager-Standardzertifikats

In Privacy Manager werden nur Privacy Manager-Zertifikate angezeigt, selbst dann, wenn zusätzliche Zertifikate von anderen Zertifizierungsstellen auf Ihrem Computer installiert sind.

Wenn Sie mehr als ein Privacy Manager-Zertifikat auf Ihrem Computer über Privacy Manager installiert haben, können Sie eines davon wie folgt als Standardzertifikat festlegen:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf das Privacy Manager-Zertifikat, das Sie als Standardzertifikat festlegen möchten, und klicken Sie dann auf **Als Standard festlegen**.
3. Klicken Sie auf **OK**.

HINWEIS: Sie müssen das Privacy Manager-Zertifikat nicht nutzen. Bei den verschiedenen Privacy Manager-Funktionen können Sie jeweils das von Ihnen gewünschte Privacy Manager-Zertifikat auswählen.

Löschen eines Privacy Manager-Zertifikats

Wenn Sie ein Privacy Manager-Zertifikat löschen, können Sie keine Dateien mehr öffnen oder Daten anzeigen, die Sie mit diesem Zertifikat verschlüsselt haben. Wenn Sie ein Privacy Manager-Zertifikat unbeabsichtigt gelöscht haben, können Sie es mithilfe der Sicherungsdatei wiederherstellen, die Sie beim Installieren des Zertifikats erstellt haben. Weitere Informationen finden Sie unter „Wiederherstellen eines Privacy Manager-Zertifikats“ auf Seite 66.

So löschen Sie ein Privacy Manager-Zertifikat:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf das Privacy Manager-Zertifikat, das sie löschen möchten, und klicken Sie anschließend auf **Erweitert**.
3. Klicken Sie auf **Löschen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
5. Klicken Sie auf **Schließen** und dann auf **Übernehmen**.

Wiederherstellen eines Privacy Manager-Zertifikats

Bei der Installation des Privacy Manager-Zertifikats müssen Sie eine Sicherungskopie des Zertifikats erstellen. Sie können auch von der Migrationsseite aus eine Sicherungskopie erstellen. Diese Sicherungskopie kann verwendet werden, wenn Sie die Anwendung auf einen anderen Computer migrieren oder ein Zertifikat auf demselben Computer wiederherstellen.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf der Seite „Migrationsdatei“ auf **Durchsuchen**, um nach der Datei mit der Erweiterung DPPSM zu suchen, die Sie während des Sicherungsprozesses erstellt haben, und klicken Sie auf **Weiter**.
4. Geben Sie das Kennwort ein, das Sie beim Erstellen der Sicherungsdatei verwendet haben, und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Fertig stellen**.

Weitere Informationen finden Sie unter „Einrichten eines Privacy Manager-Zertifikats“ auf Seite 63 oder „Sichern von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten“ auf Seite 77.

Widerrufen eines Privacy Manager-Zertifikats

Wenn Sie vermuten, dass die Sicherheit Ihres Privacy Manager-Zertifikats nicht mehr gegeben ist, können Sie Ihr eigenes Zertifikat widerrufen.

HINWEIS: Ein widerrufenes Privacy Manager-Zertifikat wird nicht gelöscht. Mithilfe des Zertifikats können auch nach dem Widerruf verschlüsselte Dateien angezeigt werden.

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Zertifikate**.
2. Klicken Sie auf **Erweitert**.
3. Klicken Sie auf das Privacy Manager-Zertifikat, das Sie widerrufen möchten, und klicken Sie anschließend auf **Widerrufen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
6. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwalten vertrauenswürdiger Kontakte

Vertrauenswürdige Kontakte sind Benutzer, mit denen Sie Privacy Manager-Zertifikate ausgetauscht haben, sodass Sie sicher mit ihnen kommunizieren können.

Mit dem Trusted Contacts Manager können Sie folgende Aufgaben ausführen:

- Anzeigen von Details zu vertrauenswürdigen Kontakten
- Löschen von vertrauenswürdigen Kontakten
- Prüfen des Widerruf-Status für vertrauenswürdige Kontakte (erweitert)

Hinzufügen von vertrauenswürdigen Kontakten

Das Hinzufügen von vertrauenswürdigen Kontakten erfolgt in drei Schritten:

1. Sie senden per E-Mail eine Einladung an vertrauenswürdige Kontakte an einen gewünschten Empfänger.
2. Der Empfänger der Einladung antwortet auf die E-Mail.
3. Sie erhalten von diesem Empfänger eine Antwort per E-Mail. Klicken Sie auf **Akzeptieren**.

Sie können Einladungen an vertrauenswürdige Kontakte per E-Mail an verschiedene Empfänger senden, oder Sie können die Einladungen an alle Kontakte in Ihrem Microsoft Outlook-Adressbuch senden.

Nachstehend erfahren Sie, wie Sie vertrauenswürdige Kontakte hinzufügen.

HINWEIS: Die Empfänger einer Einladung an vertrauenswürdige Kontakte müssen auf ihrem Computer Private Manager oder den entsprechenden Client installiert haben, um auf Ihre Einladung zu antworten und zu einem vertrauenswürdigen Kontakt zu werden. Weitere Informationen für die Installation dieses Clients finden Sie auf der DigitalPersona-Website unter http://digitalpersona.com/privacymanager/download.

Hinzufügen eines vertrauenswürdigen Kontakts

1. Öffnen Sie **Privacy Manager**, klicken Sie auf **Trusted Contacts Manager** und anschließend auf **Kontakte einladen**.

   – ODER –

   Klicken Sie in Microsoft Outlook neben **Sicher senden** in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Kontakte einladen**.

2. Nach dem Öffnen des Dialogfelds **Zertifikat auswählen** klicken Sie auf das Privacy Manager-Zertifikat, das Sie verwenden möchten. Klicken Sie abschließend auf **OK**.

3. Lesen Sie den Text im Dialogfeld **Einladung an vertrauenswürdige Kontakte**, und klicken Sie dann auf **OK**.

   Es wird automatisch eine E-Mail erzeugt.

4. Geben Sie die E-Mail-Adressen der Empfänger ein, die Sie als vertrauenswürdige Kontakte hinzufügen möchten.

5. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).

6. Klicken Sie auf **Senden**.

   HINWEIS: Wenn Sie noch kein Privacy Manager-Zertifikat erworben haben, wird eine Benachrichtigung angezeigt, dass Sie ein Privacy Manager-Zertifikat benötigen, um eine Anfrage bezüglich eines vertrauenswürdigen Kontakts zu senden. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats zu starten. Weitere Informationen finden Sie unter „Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62.

7. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   HINWEIS: Nach Erhalt muss der Empfänger der Anfrage die E-Mail öffnen und unten rechts in der E-Mail auf **Akzeptieren** und in dem daraufhin angezeigten Bestätigungsdialogfeld auf **OK** klicken.

8. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein vertrauenswürdiger Kontakt zu werden, annimmt, klicken Sie unten rechts in der E-Mail auf **Akzeptieren**.

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Liste vertrauenswürdiger Kontakte hinzugefügt wurde.

9. Klicken Sie auf **OK**.

Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte

1. Öffnen Sie Privacy Manager, klicken Sie auf **Trusted Contacts Manager** und anschließend auf **Kontakte einladen**.

   – oder –

   Klicken Sie in Microsoft Outlook neben **Sicher senden** in der Symbolleiste auf den Pfeil nach unten und anschließend auf **Meine Outlook-Kontakte einladen**.

2. Wählen Sie nach dem Öffnen der Seite „Einladung an vertrauenswürdige Kontakte“ die E-Mail-Adressen der Empfänger aus, die Sie als vertrauenswürdige Kontakte hinzufügen möchten, und klicken Sie anschließend auf **Weiter**.

3. Wenn die Seite „Einladung wird gesendet“ geöffnet wird, klicken Sie auf **Beenden**.

   Es wird automatisch eine E-Mail mit den ausgewählten Microsoft Outlook-E-Mail-Adressen erzeugt.

4. Bearbeiten Sie den Text, und unterschreiben Sie mit Ihrem Namen (optional).

5. Klicken Sie auf **Senden**.

   HINWEIS: Wenn Sie noch kein Privacy Manager-Zertifikat erworben haben, wird eine Benachrichtigung angezeigt, dass Sie ein Privacy Manager-Zertifikat benötigen, um eine Anfrage bezüglich eines vertrauenswürdigen Kontakts zu senden. Klicken Sie auf **OK**, um den Assistenten zum Anfordern eines Zertifikats zu starten. Weitere Informationen finden Sie unter „Anfordern eines Privacy Manager-Zertifikats“ auf Seite 62.

6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   HINWEIS: Nach Erhalt muss der Empfänger der Anfrage die E-Mail öffnen und unten rechts in der E-Mail auf **Akzeptieren** und in dem daraufhin angezeigten Bestätigungsdialogfeld auf **OK** klicken.

7. Wenn Sie eine E-Mail-Antwort von einem Empfänger erhalten, der die Einladung, ein vertrauenswürdiger Kontakt zu werden, annimmt, klicken Sie unten rechts in der E-Mail auf **Akzeptieren**.

   Ein Dialogfeld wird geöffnet, das bestätigt, dass der Empfänger erfolgreich zu Ihrer Liste der vertrauenswürdigen Kontakte hinzugefügt wurde.

8. Klicken Sie auf **OK**.

Anzeigen von Details zu vertrauenswürdigen Kontakten

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Vertrauenswürdige Kontakte**.
2. Klicken Sie auf einen vertrauenswürdigen Kontakt.
3. Klicken Sie auf **Kontaktdetails**.
4. Klicken Sie auf **OK**, um die Anzeige der Details zu schließen.

Löschen eines vertrauenswürdigen Kontakts

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Vertrauenswürdiger Kontakt**.
2. Klicken Sie auf den vertrauenswürdigen Kontakt, die gelöscht werden soll.
3. Klicken Sie auf **Kontakt löschen**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Prüfen des Widerruf-Status für einen vertrauenswürdigen Kontakt

So stellen Sie fest, ob ein vertrauenswürdiger Kontakt ihr Privacy Manager-Zertifikat widerrufen hat:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Vertrauenswürdiger Kontakt**.
2. Klicken Sie auf einen vertrauenswürdigen Kontakt.
3. Klicken Sie auf die Schaltfläche **Erweitert**.

Das Dialogfeld **Erweiterte Trusted Contact-Verwaltung** wird geöffnet.

4. Klicken Sie auf **Auf Widerruf prüfen**.
5. Klicken Sie auf **Schließen**.

Allgemeine Aufgaben

Sie können Privacy Manager mit den folgenden Microsoft Produkten verwenden:

- Microsoft Outlook
- Microsoft Office

Verwenden von Privacy Manager in Microsoft Outlook

Nach der Installation von Privacy Manager wird die Schaltfläche „Datenschutz“ auf der Symbolleiste von Microsoft Outlook angezeigt, und die Schaltfläche „Sichern senden“ wird auf der Symbolleiste jeder E-Mail-Nachricht in Microsoft Outlook angezeigt. Wenn Sie neben **Datenschutz** oder **Sicher senden** auf den Pfeil nach unten klicken, können Sie zwischen folgenden Optionen auswählen:

- **Nachricht signieren und senden** (nur für die Schaltfläche „Sicher senden“) – Diese Option fügt Ihrer E-Mail eine digitale Signatur hinzu und versendet sie, sobald die Authentifizierung über die von Ihnen ausgewählte Sicherheits-Anmeldemethode erfolgt ist.
- **Für vertrauenswürdige Kontakte versiegeln und senden** (nur für die Schaltfläche „Sicher senden“) – Diese Option fügt Ihrer E-Mail eine digitale Signatur hinzu, verschlüsselt sie und versendet die E-Mail, sobald die Authentifizierung über die von Ihnen ausgewählte Sicherheits-Anmeldemethode erfolgt ist.
- **Kontakte einladen** – Mit dieser Option können Sie eine Einladung an vertrauenswürdige Kontakte versenden. Weitere Informationen finden Sie unter „Hinzufügen eines vertrauenswürdigen Kontakts“ auf Seite 68.
- **Meine Outlook-Kontakte einladen** – Mit dieser Option können Sie eine Einladung an alle Kontakte in Ihrem Microsoft Outlook-Adressbuch senden. Weitere Informationen finden Sie unter „Hinzufügen von vertrauenswürdigen Kontakten unter Verwendung der Microsoft Outlook-Kontakte“ auf Seite 68.
- **Privacy Manager–Software öffnen** – Mit Zertifikaten, vertrauenswürdigen Kontakten und Einstellungsoptionen können Sie die Privacy Manager-Software öffnen, um aktuelle Einstellungen hinzuzufügen, anzuzeigen oder zu aktualisieren. Weitere Informationen finden Sie unter „Verwalten von Privacy Manager Zertifikaten“ auf Seite 62, „Verwalten vertrauenswürdiger Kontakte“ auf Seite 67 oder „Konfigurieren von Privacy Manager für Microsoft Outlook“ auf Seite 71.

Konfigurieren von Privacy Manager für Microsoft Outlook

1. Öffnen Sie **Privacy Manager**, klicken Sie auf **Einstellungen** und anschließend auf die Registerkarte **E-Mail**.

   – ODER –

   Klicken Sie in der Hauptsymbolleiste von Microsoft Outlook neben **Sicher senden** (**Datenschutz** in Outlook 2003) auf den Pfeil nach unten und anschließend auf **Einstellungen**.

   – ODER –

   Klicken Sie in der Symbolleiste einer Microsoft Outlook-E-Mail-Nachricht neben **Sicher senden** auf den Pfeil nach unten und anschließend auf **Einstellungen**.

2. Wählen Sie die Aktionen aus, die ausgeführt werden sollen, wenn Sie eine sichere E-Mail senden, und klicken Sie anschließend auf **OK**.

Signieren und Senden einer E-Mail-Nachricht

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Klicken Sie neben **Sicher senden** (**Datenschutz** in Outlook 2003) auf den Pfeil nach unten und anschließend auf **Signieren und senden**.
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Versiegeln und Senden einer E-Mail-Nachricht

Versiegelte E-Mail-Nachrichten, die digital signiert und versiegelt (verschlüsselt) sind, können nur von den Personen angezeigt werden, die Sie aus Ihrer Liste der vertrauenswürdigen Kontakte ausgewählt haben.

So versiegeln und senden Sie eine E-Mail-Nachricht an einen vertrauenswürdigen Kontakt:

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Klicken Sie neben **Sicher senden** auf den Pfeil nach unten (**Datenschutz** in Outlook 2003) und anschließend auf **Für vertrauenswürdige Kontakte versiegeln und senden**.
4. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Anzeigen einer versiegelten E-Mail-Nachricht

Wenn Sie eine versiegelte E-Mail-Nachricht öffnen, wird das Sicherheits-Label im Kopf der E-Mail angezeigt. Das Sicherheits-Label enthält die folgenden Informationen:

- die Anmeldeinformationen, die zur Überprüfung der Identität der Person verwendet wurden, die die E-Mail signiert hat
- das Produkt, das zur Überprüfung der Anmeldeinformationen der Person verwendet wurde, die die E-Mail signiert hat

Verwenden von Privacy Manager in einem Microsoft Office 2007 Dokument

Nach der Installation Ihres Privacy Manager-Zertifikats wird die Schaltfläche „Signieren und verschlüsseln“ rechts in der Symbolleiste aller Microsoft Word-, Microsoft Excel- und Microsoft PowerPoint-Dokumente angezeigt. Wenn Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten klicken, können Sie eine der folgenden Optionen auswählen:

- **Dokument signieren** – Mithilfe dieser Option können Sie Ihre digitale Signatur zu dem Dokument hinzufügen.
- **Signaturzeile vor Signieren hinzufügen** (nur für Microsoft Word und Microsoft Excel) – Beim Signieren oder Verschlüsseln eines Microsoft Word- oder Microsoft Excel-Dokuments wird standardmäßig eine Signaturzeile hinzugefügt. Zum Deaktivieren dieser Optionen klicken Sie auf **Signaturzeile hinzufügen**, und entfernen Sie das Häkchen.
- **Dokument verschlüsseln** – Mithilfe dieser Option können Sie Ihre digitale Signatur zu dem Dokument hinzufügen und es verschlüsseln.

- **Verschlüsselung entfernen** – Mithilfe dieser Option entfernen Sie die Verschlüsselung des Dokuments.
- **Privacy Manager–Software öffnen** – Mit Zertifikaten, vertrauenswürdigen Kontakten und Einstellungsoptionen können Sie die Privacy Manager-Software öffnen, um aktuelle Einstellungen hinzuzufügen, anzuzeigen oder zu aktualisieren. Weitere Informationen finden Sie unter „Verwalten von Privacy Manager Zertifikaten“ auf Seite 62, „Verwalten vertrauenswürdiger Kontakte“ auf Seite 67 oder „Konfigurieren von Privacy Manager für Microsoft Office“ auf Seite 73.

Konfigurieren von Privacy Manager für Microsoft Office

1. Öffnen Sie **Privacy Manager**, klicken Sie auf **Einstellungen** und anschließend auf die Registerkarte **Dokumente**.

   – ODER –

   Klicken Sie in der Symbolleiste eines Microsoft Office-Dokuments neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Einstellungen**.
2. Wählen Sie die Aktionen aus, die Sie konfigurieren möchten, und klicken Sie anschließend auf **OK**.

Signieren eines Microsoft Office-Dokuments

1. Erstellen Sie in Microsoft Word, Microsoft Excel oder Microsoft PowerPoint ein Dokument, und speichern Sie es.
2. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Dokument signieren**.
3. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
4. Lesen Sie den Text im Bestätigungsdialogfeld, und klicken Sie dann auf **OK**.

Wenn Sie das Dokument später bearbeiten möchten, müssen Sie wie folgt vorgehen:

1. Klicken Sie auf die Schaltfläche **Office** links oben auf dem Bildschirm.
2. Klicken Sie auf **Erstellen** und dann auf **Als endgültig markieren**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**, und fahren Sie mit Ihrer Arbeit fort.
4. Wenn Sie die Bearbeitung abgeschlossen haben, signieren Sie das Dokument erneut.

Hinzufügen einer Signaturzeile beim Signieren eines Microsoft Word- oder Microsoft Excel-Dokuments

Mit Privacy Manager können Sie eine Signaturzeile hinzufügen, wenn Sie ein Microsoft Word- oder Microsoft Excel-Dokument signieren:

1. Erstellen oder speichern Sie ein Dokument in Microsoft Word oder Microsoft Excel.
2. Klicken Sie auf das Menü **Startseite**.
3. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Signaturzeile vor Signieren hinzufügen**.

HINWEIS: Bei aktivierter Option ist das Kontrollkästchen neben „Signaturzeile vor Signieren hinzufügen“ markiert. Diese Option ist standardmäßig aktiviert.

4. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten und anschließend auf **Dokument signieren**.

5. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

Hinzufügen eines empfohlenen Signierers zu einem Microsoft Word- oder Microsoft Excel-Dokument

Sie können mehr als eine Signaturzeile zu Ihrem Dokument hinzufügen, indem Sie empfohlene Signierer bestimmen. Bei einem empfohlenen Signierer handelt es sich um einen Benutzer, der von dem Eigentümer eines Microsoft Word- oder Microsoft Excel-Dokuments dazu bestimmt wird, dem Dokument eine Signaturzeile hinzuzufügen. Der empfohlene Signierer können entweder Sie selbst sein oder eine andere Person, die Ihr Dokument für Sie signieren soll. Wenn sie z. B. ein Dokument vorbereiten, das von allen Mitgliedern Ihrer Abteilung signiert werden soll, können Sie Signaturzeilen für diese Benutzer unten auf der letzten Seite des Dokuments mit der Angabe einfügen, bis zu welchem Datum das Dokument signiert werden muss.

So fügen Sie einen empfohlenen Signierer zu einem Microsoft Word- oder Microsoft Excel-Dokument hinzu:

1. Erstellen Sie in Microsoft Word oder Microsoft Excel ein Dokument, und speichern Sie es.

2. Klicken Sie auf das Menü **Einfügen**.

3. Klicken Sie in der Gruppe **Text** in der Symbolleiste neben **Signaturzeile** auf den Pfeil nach unten und anschließend auf **Privacy Manager Signature Provider**.

   Das Dialogfeld „Einrichten der Signatur“ wird geöffnet.

4. Geben Sie in das Feld unter **Empfohlener Signierer** den Namen des empfohlenen Signierers ein.

5. Geben Sie in das Feld unter **Anleitungen für Signierer** eine Mitteilung für diesen empfohlenen Signierer ein.

   HINWEIS: Diese Mitteilung wird anstelle eines Titels angezeigt und nach dem Signieren entweder gelöscht oder durch den Titel des Benutzers ersetzt.

6. Markieren Sie das Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen**, um das Datum anzuzeigen.

7. Markieren Sie das Kontrollkästchen **Titel des Signierers in Signaturzeile anzeigen**, um den Titel anzuzeigen.

   HINWEIS: Der Eigentümer des Dokuments weist seinem Dokument empfohlene Signierer zu. Die Kontrollkästchen **Signierungsdatum in Signaturzeile anzeigen** und/oder **Titel des Signierers in Signaturzeile anzeigen** müssen aktiviert sein, damit der empfohlene Signierer das Datum und/oder den Titel in der Signaturzeile anzeigen kann.

8. Klicken Sie auf **OK**.

Hinzufügen der Signaturzeile eines empfohlenen Signierers

Wenn empfohlene Signierer das Dokument öffnen, sehen sie ihren Namen in Klammern; das bedeutet, dass ihre Signatur erforderlich ist.

So signieren Sie das Dokument:

1. Doppelklicken Sie auf die entsprechende Signaturzeile.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.

   Die Signaturzeile wird gemäß den Einstellungen angezeigt, die der Eigentümer des Dokuments festgelegt hat.

Verschlüsseln eines Microsoft Office-Dokuments

Sie können ein Microsoft Office-Dokument für sich selbst und für Ihre vertrauenswürdigen Kontakte verschlüsseln. Nachdem Sie ein Dokument verschlüsselt und geschlossen haben, muss es von Ihnen und den aus der Liste ausgewählten vertrauenswürdigen Kontakten authentifiziert werden, bevor es erneut geöffnet werden kann.

So verschlüsseln Sie ein Microsoft Office-Dokument:

1. Erstellen Sie in Microsoft Word, Microsoft Excel oder Microsoft PowerPoint ein Dokument, und speichern Sie es.
2. Klicken Sie auf das Menü **Startseite**.
3. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten, und klicken Sie anschließend auf **Dokument verschlüsseln**.

   Das Dialogfeld **Vertrauenswürdigen Kontakt auswählen** wird geöffnet.
4. Klicken Sie auf den Namen eines vertrauenswürdigen Kontakts, der in der Lage sein soll, das Dokument zu öffnen und seinen Inhalt anzuzeigen.

   HINWEIS: Um mehrere Namen vertrauenswürdiger Kontakte auszuwählen, drücken Sie die Taste strg, und klicken Sie anschließend auf die Namen der entsprechenden Personen.
5. Klicken Sie auf **OK**.

Für ein späteres Überarbeiten des Dokuments folgen Sie der Anleitung unter „Eine Verschlüsselung von einem Microsoft Office-Dokument entfernen“ auf Seite 75. Sie können das Dokument überarbeiten, nachdem die Verschlüsselung entfernt wurde. Zur erneuten Verschlüsselung des Dokuments folgen Sie der Anleitung in diesem Abschnitt.

Eine Verschlüsselung von einem Microsoft Office-Dokument entfernen

Wenn Sie die Verschlüsselung für ein Microsoft Office-Dokument entfernen, ist weder für Sie noch für Ihre vertrauenswürdigen Kontakte eine Authentifizierung erforderlich, um das Dokument zu öffnen und seinen Inhalt anzuzeigen.

So entfernen Sie die Verschlüsselung für ein Microsoft Office-Dokument

1. Öffnen Sie ein verschlüsseltes Microsoft Word-, Microsoft Excel- oder Microsoft PowerPoint-Dokument.
2. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
3. Klicken Sie auf das Menü **Startseite**.
4. Klicken Sie neben **Signieren und verschlüsseln** auf den Pfeil nach unten, und klicken Sie anschließend auf **Verschlüsselung entfernen**.

Versenden eines verschlüsselten Microsoft Office-Dokuments

Sie können ein verschlüsseltes Microsoft Office-Dokument an eine E-Mail-Nachricht anhängen, ohne dabei die E-Mail selbst zu signieren oder zu verschlüsseln. Sie erstellen und senden eine E-Mail mit einem signierten oder verschlüsselten Dokument als Anhang genau so, wie Sie eine reguläre E-Mail mit Anhang versenden würden.

Für optimale Sicherheit empfiehlt es sich jedoch, die E-Mail zu verschlüsseln, wenn ein signiertes oder verschlüsseltes Microsoft Office-Dokument angehängt wird.

Gehen Sie folgendermaßen vor, um eine versiegelte E-Mail zu versenden, an die ein signiertes und/ oder verschlüsseltes Microsoft Office-Dokument angehängt ist:

1. Klicken Sie in Microsoft Outlook auf **Neu** oder **Antworten**.
2. Schreiben Sie Ihre E-Mail-Nachricht.
3. Hängen Sie das Microsoft Office-Dokument an.
4. Weitere Informationen erhalten Sie unter „Versiegeln und Senden einer E-Mail-Nachricht“ auf Seite 72.

Anzeigen eines signierten Microsoft Office-Dokuments

HINWEIS: Sie müssen kein Privacy Manager-Zertifikat besitzen, um ein signiertes Microsoft Office-Dokument anzuzeigen.

Beim Öffnen eines signierten Microsoft Office-Dokuments wird das Symbol für digitale Signaturen in der Statusleiste unten im Dokumentfenster angezeigt.

1. Klicken Sie auf das Symbol **Digitale Signatur**, um auf die Anzeige des Signatur-Dialogfelds umzuschalten, in dem die Namen aller Benutzer angezeigt werden, die das Dokument signiert haben, sowie das Datum, an dem die einzelnen Signaturen vorgenommen wurden.
2. Weitere Details zu den einzelnen Signaturen werden angezeigt, wenn Sie mit der rechten Maustaste auf einen Namen im Signatur-Dialogfelds klicken und dann **Signaturdetails** auswählen.

Anzeigen eines verschlüsselten Microsoft Office-Dokuments

Zum Anzeigen eines verschlüsselten Microsoft Office-Dokuments auf einem anderen Computer muss Privacy Manager auf diesem Computer installiert sein. Darüber hinaus müssen Sie das Privacy Manager-Zertifikat wiederherstellen, das für die Verschlüsselung der Datei verwendet wurde.

Wenn Ihr Zertifikat verloren gegangen ist, müssen Sie das zur Verschlüsselung der Datei verwendete Privacy Manager-Zertifikat wiederherstellen, um ein verschlüsseltes Microsoft Office-Dokument anzeigen zu können.

Ein vertrauenswürdiger Kontakt, der ein verschlüsseltes Microsoft Office Dokument anzeigen möchte, muss über ein installiertes Privacy Manager Zertifikat sowie über Privacy Manager auf ihrem Computer verfügen. Außerdem muss der vertrauenswürdige Kontakt vom Eigentümer des verschlüsselten Microsoft Office Dokuments ausgewählt worden sein.

Erweiterte Aufgaben

Migrieren von Privacy Manager Zertifikaten und vertrauenswürdigen Kontakten en auf einen anderen Computer

Sie können Ihre Privacy Manager-Zertifikate und vertrauenswürdigen Kontakte sicher auf einen anderen Computer migrieren oder Sicherungskopien Ihrer Daten anlegen. Sichern Sie dazu die Privacy Manager-Zertifikate und die vertrauenswürdigen Kontakte als kennwortgeschützte Datei in einen Netzwerkordner oder auf einen Wechseldatenträger, und stellen Sie anschließend die Datei auf dem neuen Computer wieder her.

Sichern von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager-Zertifikate und vertrauenswürdigen Kontakte in einer kennwortgeschützten Datei zu sichern:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Sicherung**.
3. Wählen Sie auf der Seite „Daten auswählen“ die Datenkategorien aus, die in die Migrationsdatei mit aufgenommen werden sollen, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie auf der Seite „Migrationsdatei“ einen Dateinamen ein, oder klicken Sie auf **Durchsuchen**, um nach einem Speicherort zu suchen. Klicken Sie anschließend auf **Weiter**.
5. Geben Sie ein Kennwort ein, bestätigen Sie es, und klicken Sie auf **Weiter**.

   HINWEIS: Bewahren Sie dieses Kennwort an einem sicheren Ort auf, da Sie zum Wiederherstellen der Migrationsdatei benötigen.

6. Authentifizieren Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode.
7. Klicken Sie auf der Seite „Migrationsdatei gespeichert“ auf **Beenden**.

Wiederherstellen von Privacy Manager-Zertifikaten und vertrauenswürdigen Kontakten

Gehen Sie folgendermaßen vor, um Ihre Privacy Manager-Zertifikate und vertrauenswürdigen Kontakte als Teil des Migrationsprozesses auf einem anderen Computer oder auf demselben Computer wiederherzustellen:

1. Öffnen Sie Privacy Manager, und klicken Sie dann auf **Migration**.
2. Klicken Sie auf **Wiederherstellen**.
3. Klicken Sie auf der Seite „Migrationsdatei“ auf **Durchsuchen**, um nach der Datei zu suchen. Klicken Sie anschließend auf **Weiter**.
4. Geben Sie das Kennwort ein, das Sie beim Erstellen der Sicherungsdatei verwendet haben, und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite „Migrationsdatei“ auf **Beenden**.

Zentrale Verwaltung von Privacy Manager

Bei Ihrer Installation von Privacy Manager kann es sich um einen Teil einer zentralen Installation handeln, die von Ihrem Administrator benutzerdefiniert angepasst wurde. Eine oder mehrere der folgenden Funktionen können entweder aktiviert oder deaktiviert sein:

- **Richtlinien zur Zertifikatsverwendung** – Es kann eine Beschränkung auf die Verwendung von Privacy Manager-Zertifikaten vorliegen, die von Comodo ausgegeben wurden, oder Sie können zur Nutzung digitaler Zertifikate anderer Zertifizierungsstellen berechtigt sein.
- **Verschlüsselungsrichtlinien** – Verschlüsselungsfunktionen können in Microsoft Office oder Outlook individuell aktiviert oder deaktiviert werden.

7 File Sanitizer for HP ProtectTools

Mit File Sanitizer können Sie Datenbestände auf Ihrem Computer (z. B. persönliche Daten oder Dateien, Verlaufsdaten, Internet-bezogene und anderweitige Daten) sicher shreddern und von Zeit zu Zeit die Daten auf Ihrer Festplatte überschreiben.

HINWEIS: Die vorliegende Version von File Sanitizer unterstützt lediglich das Überschreiben der Computerfestplatte.

Shreddern

Das Shreddern von Daten ist nicht mit einem Standard-Löschvorgang unter Windows® gleichzusetzen; dieser Vorgang wird in File Sanitizer als „einfaches Löschen" bezeichnet. Beim Shreddern von Datenbeständen mit File Sanitizer werden die Dateien mit bedeutungslosen Daten überschrieben. Damit ist quasi ausgeschlossen, dass der ursprüngliche Datenbestand wiederhergestellt werden kann. Bei einem Löschvorgang unter Windows verbleiben die Dateien bzw. Datenbestände dagegen auf der Festplatte oder können anhand datenforensischer Methoden wiedergewonnen werden.

Wenn Sie ein Shred-Profil auswählen (**Hohe Sicherheit**, **Mittlere Sicherheit** oder **Geringe Sicherheit**), wird für das Shreddern automatisch eine voreingestellte Liste von Datenbeständen sowie eine Löschmethode ausgewählt. Sie können ein Shred-Profil auch individuell anpassen. Dabei können Sie die Anzahl der Shred-Zyklen festlegen und angeben, welche Datenbestände geshreddert werden sollen bzw. welche Datenbestände nur nach vorheriger Bestätigung oder überhaupt nicht geshreddert werden sollen. Weitere Informationen finden Sie unter „Auswählen und Ändern eines Shred-Profils" auf Seite 84.

Sie können einen automatischen Shred-Zeitplan erstellen oder das Shreddern manuell mithilfe des Symbols **HP ProtectTools** aktivieren, das sich im Infobereich ganz rechts in der Taskleiste befindet. Weitere Informationen finden Sie unter „Festlegen eines Shred-Zeitplans" auf Seite 83, „Manuelles Shreddern von Datenbeständen" auf Seite 88 oder „Manuelles Shreddern aller ausgewählter Elemente" auf Seite 89.

HINWEIS: .dll-Dateien werden nur dann geshreddert und vom System entfernt, wenn sie zuvor in den Papierkorb verschoben wurden.

Überschreiben von freiem Speicherplatz

Das Löschen eines Datenbestands in Windows entfernt den Inhalt des betreffenden Datenbestands nicht vollständig von der Festplatte. Windows löscht lediglich den Verweis zu dem Datenbestand. Der Inhalt ist auch weiterhin auf der Festplatte vorhanden, bis ein anderer Datenbestand denselben Bereich auf der Festplatte mit neuen Informationen überschreibt.

Beim Überschreiben von freiem Speicherplatz werden gelöschte Datenbestände sicher mit willkürlichen Daten überschrieben, sodass die Originalinhalte nicht mehr angezeigt werden können.

HINWEIS: Das Überschreiben von freiem Speicherplatz kann von Zeit zu Zeit für Datenbestände erfolgen, die Sie mit der File Sanitizer Option **Einstellungen für einfaches Löschen**, durch Verschieben in den Papierkorb oder manuell gelöscht haben. Das Überschreiben von freiem Speicherplatz bietet keine zusätzliche Sicherheit für geshredderte Datenbestände.

Sie können einen Zeitplan für das automatische Überschreiben von freiem Speicherplatz erstellen oder das Überschreiben manuell mithilfe des Symbols **HP ProtectTools** aktivieren, das sich im Infobereich ganz rechts in der Taskleiste befindet. Weitere Informationen finden Sie unter „Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz“ auf Seite 83 oder „Manuelles Aktivieren des Überschreibens von freiem Speicherplatz“ auf Seite 89.

Öffnen von File Sanitizer

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie auf **File Sanitizer**.

– oder –

▲ Doppelklicken Sie auf das **File Sanitizer**-Symbol auf dem Desktop.

– oder –

▲ Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich ganz rechts in der Taskleiste. Klicken Sie auf **File Sanitizer** und anschließend auf **File Sanitizer öffnen**.

Setup-Verfahren

Festlegen eines Shred-Zeitplans

Sie können ein vordefiniertes Shred-Profil auswählen oder Ihr eigenes Profil erstellen. Weitere Informationen finden Sie unter „Auswählen und Ändern eines Shred-Profils“ auf Seite 84. Datenbestände lassen sich außerdem jederzeit manuell shreddern. Weitere Informationen finden Sie unter „Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs“ auf Seite 87.

HINWEIS: Eingeplante Aufgaben werden zu einem bestimmten Zeitpunkt durchgeführt. Wenn das System zu diesem Zeitpunkt ausgeschaltet ist oder sich im Standby- oder Energiesparmodus befindet, versucht File Sanitizer nicht, die Aufgabe zu einem späteren Zeitpunkt durchzuführen.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Wählen Sie die gewünschten Shred-Optionen aus:
   - **Beim Herunterfahren von Windows** – Shreddert alle ausgewählten Datenbestände beim Herunterfahren von Windows.

     HINWEIS: Beim Herunterfahren wird ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie mit dem Shreddern ausgewählter Datenbestände fortfahren oder den Vorgang übergehen möchten.

     Klicken Sie auf **Ja**, um das Shreddern zu übergehen, bzw. auf **Nein**, wenn die Daten geshreddert werden sollen.
   - **Beim Öffnen eines Webbrowsers** – Shreddert beim Öffnen eines Webbrowsers alle Internet-bezogenen Datenbestände, wie beispielsweise das URL-Protokoll des Browsers.
   - **Beim Schließen eines Webbrowsers** – Shreddert beim Schließen eines Webbrowsers alle Internet-bezogenen Datenbestände, wie beispielsweise das URL-Protokoll des Browsers.
   - **Tastenfolge** – Ermöglicht die Definition einer Tastenfolge, die den Shred-Vorgang einleitet. Ausführliche Informationen zu diesem Thema finden Sie unter „Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs“ auf Seite 87.

   HINWEIS: .dll-Dateien werden nur dann geshreddert und vom System entfernt, wenn sie zuvor in den Papierkorb verschoben wurden.
3. Wenn Sie ausgewählte Datensätze zu einem späteren Zeitpunkt shreddern möchten, aktivieren Sie das Kontrollkästchen **Planer aktivieren**, geben Ihr Windows Kennwort ein und wählen dann einen Tag und eine Uhrzeit aus.
4. Klicken Sie auf **Übernehmen**.

Erstellen eines Zeitplans für das Überschreiben von freiem Speicherplatz

Das Überschreiben von freiem Speicherplatz kann von Zeit zu Zeit für Datenbestände erfolgen, die Sie mit der File Sanitizer Option **Einstellungen für einfaches Löschen**, durch Verschieben in den Papierkorb oder manuell gelöscht haben. Das Überschreiben von freiem Speicherplatz bietet keine zusätzliche Sicherheit für geshredderte Datenbestände.

HINWEIS: Eingeplante Aufgaben werden zu einem bestimmten Zeitpunkt durchgeführt. Wenn das System zu diesem Zeitpunkt ausgeschaltet ist oder sich im Standby- oder Energiesparmodus befindet, versucht File Sanitizer nicht, die Aufgabe zu einem späteren Zeitpunkt durchzuführen.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Überschreiben**.
2. Wenn Sie gelöschte Bestände auf Ihrer Festplatte zu einem späteren Zeitpunkt überschreiben möchten, aktivieren Sie das Kontrollkästchen **Planer aktivieren**, geben Ihr Windows Kennwort ein und wählen dann einen Tag und eine Uhrzeit aus.
3. Klicken Sie auf **Übernehmen**.

HINWEIS: Das Überschreiben von freiem Speicherplatz kann einige Zeit in Anspruch nehmen. Obwohl der Vorgang im Hintergrund ausgeführt wird, kann die Computerleistung durch die zusätzliche Prozessorbelastung beeinträchtigt werden.

Auswählen und Ändern eines Shred-Profils

Sie können eine Löschmethode festlegen und die zu shreddernden Datenbestände auswählen, indem Sie ein vordefiniertes Profil auswählen oder Ihr eigenes Profil erstellen.

Auswählen eines vordefinierten Shred-Profils

Wenn Sie ein vordefiniertes Shred-Profil auswählen, werden automatisch eine vordefinierte Löschmethode und eine Liste von Datenbeständen ausgewählt. Sie können die vordefinierte Liste der für das Shreddern vorgesehenen Datenbestände anzeigen lassen.

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Einstellungen**.
2. Klicken Sie auf ein vordefiniertes Shred-Profil:
   - **Hohe Sicherheit**
   - **Mittlere Sicherheit**
   - **Geringe Sicherheit**
3. Zur Anzeige der für das Shreddern vorgesehenen Datenbestände klicken Sie auf **Details anzeigen**.
   a. **Ausgewählte Elemente werden geshreddert, und eine Bestätigungsmeldung wird angezeigt. Nicht ausgewählte Elemente werden geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.** – Wählen Sie das Kontrollkästchen aus, um eine Bestätigungsmeldung anzuzeigen, bevor das Element geshreddert wird. Wenn Sie das Kontrollkästchen nicht auswählen, wird das Element geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.

      HINWEIS: Auch wenn das Kontrollkästchen für ein Element nicht angekreuzt ist, wird das Element geshreddert.

   b. Klicken Sie auf **Übernehmen**.
4. Klicken Sie auf **Übernehmen**.

Anpassen eines Shred-Profils

Beim Erstellen eines Shred-Profils können Sie die folgenden Informationen angeben: Anzahl der Shred-Zyklen, welche Datenbestände in den Shred-Vorgang einbezogen werden sollen, für welche

Datenbestände das Shreddern vor dem Ausführen des Befehls bestätigt werden soll und welche Datenbestände vom Shred-Prozess ausgeschlossen werden sollen.

1. Öffnen Sie File Sanitizer, klicken Sie auf **Einstellungen**, **Einstellungen für erhöhte Sicherheit** und anschließend auf **Details anzeigen**.

2. Wählen Sie die Anzahl der Shred-Zyklen aus.

   HINWEIS: Der ausgewählte Wert legt fest, wie häufig der Shred-Zyklus auf die einzelnen Datenbestände angewendet wird. So wird der Shred-Algorithmus bei Auswahl von „3“ insgesamt drei Mal ausgeführt. Wenn Sie sich für eine höhere Sicherheit mit häufigeren Shred-Zyklen entscheiden, kann der Shred-Vorgang erheblich länger dauern. Allerdings wird es mit steigender Anzahl der Shred-Zyklen immer schwieriger, die Daten wiederherzustellen, so dass die Sicherheit zunimmt.

3. So wählen Sie die zu shreddernden Datenbestände aus:

   a. Klicken Sie unter **Verfügbare Shred-Optionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.

   b. Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Benutzerdefinierte Option hinzufügen**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein.

   c. Klicken Sie auf **Öffnen** und dann auf **OK**.

   d. Klicken Sie unter **Verfügbare Shred-Optionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.

   Zum Löschen eines Datenbestands aus den verfügbaren Shred-Optionen klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

4. **Ausgewählte Elemente werden geshreddert, und eine Bestätigungsmeldung wird angezeigt. Nicht ausgewählte Elemente werden geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.** – Wählen Sie das Kontrollkästchen aus, um eine Bestätigungsmeldung anzuzeigen, bevor das Element geshreddert wird. Wenn Sie das Kontrollkästchen nicht auswählen, wird das Element geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.

   HINWEIS: Auch wenn das Kontrollkästchen für ein Element nicht angekreuzt ist, wird das Element geshreddert.

   Zum Entfernen eines Datenbestands aus der Shred-Liste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Entfernen**.

5. So schließen Sie Dateien und Ordner vom automatischen Shreddern aus:

   a. Klicken Sie unter **Folgende Elemente nicht shreddern** auf **Hinzufügen**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein.

   b. Klicken Sie auf **Öffnen** und dann auf **OK**.

   Zum Löschen eines Datenbestands aus der Ausschlussliste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

6. Klicken Sie auf **Übernehmen**.

Anpassen eines Profils für das einfache Löschen

Das Profil für einfaches Löschen umfasst das standardmäßige Löschen von Datenbeständen ohne Shreddern der Daten. Sie können ein Profil für das einfache Löschen auch individuell anpassen. Dabei können Sie angeben, welche Datenbestände gelöscht werden sollen, für welche Datensätze vor dem Löschen eine Bestätigung notwendig ist, und welche Datensätze nicht gelöscht werden sollen.

HINWEIS: Mit der Option **Einstellungen für einfaches Löschen** können Sie das Bereinigen der Festplatte von Zeit zu Zeit für Datenbestände durchführen, die Sie über den Windows Papierkorb oder manuell gelöscht haben.

1. Öffnen Sie File Sanitizer, klicken Sie auf **Einstellungen**, **Einstellungen für einfaches Löschen** und anschließend auf **Details anzeigen**.

2. Wählen Sie die zu löschenden Datenbestände aus:

   a. Klicken Sie unter **Verfügbare Löschoptionen** auf einen Datenbestand und anschließend auf **Hinzufügen**.

   b. Zum Hinzufügen eines benutzerdefinierten Datenbestands klicken Sie auf **Benutzerdefinierte Option hinzufügen**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein. Klicken Sie abschließend auf **OK**.

   c. Klicken Sie auf den benutzerdefinierten Datenbestand und anschließend auf **Hinzufügen**.

   Zum Entfernen eines Datenbestands aus den verfügbaren Löschoptionen klicken Sie auf den betreffenden Datenbestand und dann auf **Löschen**.

3. **Ausgewählte Elemente werden geshreddert, und eine Bestätigungsmeldung wird angezeigt. Nicht ausgewählte Elemente werden geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.** – Wählen Sie das Kontrollkästchen aus, um eine Bestätigungsmeldung anzuzeigen, bevor das Element geshreddert wird. Wenn Sie das Kontrollkästchen nicht auswählen, wird das Element geshreddert, ohne dass eine Bestätigungsmeldung angezeigt wird.

   HINWEIS: Auch wenn das Kontrollkästchen für ein Element nicht angekreuzt ist, wird das Element geshreddert.

   Zum Entfernen eines Datenbestands aus der Liste der zu löschenden Datenbestände klicken Sie auf den betreffenden Datenbestand und anschließend auf **Entfernen**.

4. So schließen Sie Datenbestände vom automatischen Löschen aus:

   a. Klicken Sie unter **Folgende Elemente nicht löschen** auf **Hinzufügen**. Suchen Sie dann den Pfad zu der Datei oder dem Ordner, oder tippen Sie ihn ein.

   b. Klicken Sie auf **Öffnen** und dann auf **OK**.

   Zum Löschen eines Datenbestands aus der Ausschlussliste klicken Sie auf den betreffenden Datenbestand und anschließend auf **Löschen**.

5. Klicken Sie auf **Übernehmen**.

Allgemeine Aufgaben

Sie können mit File Sanitizer die folgenden Aufgaben ausführen:

- Einleiten des Shred-Vorgangs über eine Tastenfolge – Mit dieser Funktion können Sie eine Tastenfolge (z. B. strg+alt+s) zum Einleiten des Shred-Vorgangs festlegen. Nähere Informationen zu diesem Thema finden Sie unter „Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs“ auf Seite 87.
- Einleiten des Shred-Vorgangs über das Symbol „File Sanitizer“ – Diese Funktion ist vergleichbar mit der Funktion Ziehen und Ablegen unter Windows. Nähere Informationen zu diesem Thema finden Sie unter „Verwenden des File Sanitizer-Symbols“ auf Seite 88.
- Manuelles Shreddern eines bestimmten Datenbestands oder aller ausgewählten Datenbestände – Diese Funktionen ermöglichen das manuelle Shreddern außerhalb des Shred-Zeitplans. Nähere Informationen zu diesem Thema finden Sie unter „Manuelles Shreddern von Datenbeständen“ auf Seite 88 oder „Manuelles Shreddern aller ausgewählter Elemente“ auf Seite 89.
- Manuelles Aktivieren des Überschreibens von freiem Speicherplatz – Mithilfe dieser Funktion können Sie das Überschreiben von freiem Speicherplatz auf der Festplatte manuell aktivieren. Nähere Informationen zu diesem Thema finden Sie unter „Manuelles Aktivieren des Überschreibens von freiem Speicherplatz“ auf Seite 89.
- Abbrechen eines Shred-Vorgangs oder einer Überschreibung von freiem Speicherplatz – Über diese Funktion haben Sie die Möglichkeit, den aktuellen Shred-Vorgang oder das Überschreiben von freiem Speicherplatz auf der Festplatte abzubrechen. Nähere Informationen zu diesem Thema finden Sie unter „Abbrechen eines Shred- oder Überschreibungsvorgangs“ auf Seite 89.
- Anzeigen der Protokolldateien – Mit dieser Funktion zeigen Sie die Protokolldateien für Shred-Vorgänge und Überschreibungsvorgänge von freiem Speicherplatz an, die sämtliche Fehler für den letzten Shred-Vorgang bzw. die letzte Überschreibung von freiem Speicherplatz enthalten. Nähere Informationen zu diesem Thema finden Sie unter „Anzeigen der Protokolldateien“ auf Seite 89.

HINWEIS: Der Shred-Vorgang oder die Überschreibung von freiem Speicherplatz kann viel Zeit in Anspruch nehmen. Auch wenn das Shreddern und das Überschreiben im Hintergrund stattfinden, wird die Verarbeitungsleistung Ihres Computers unter Umständen durch die erhöhte Prozessorbeanspruchung beeinträchtigt.

Verwenden einer Tastenfolge zur Einleitung des Shred-Vorgangs

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Aktivieren Sie das Kontrollkästchen **Tastenfolge**.
3. Geben Sie ein Zeichen in das entsprechende Feld ein.
4. Markieren Sie das Kontrollkästchen **STRG** oder **ALT**, und markieren Sie dann die Option **UMSCHALTTASTE**.

   Um zum Beispiel das automatische Shreddern mit der Tastenfolge s und strg+Umschalttaste auszulösen, geben Sie in das dafür vorgesehene Feld den Buchstaben s ein und markieren die Kontrollkästchen **STRG** und **UMSCHALTTASTE**.

HINWEIS: Achten Sie darauf, keine bereits für andere Zwecke konfigurierte Tastenfolge zu verwenden.

So leiten Sie den Shred-Vorgang mit einer Tastenfolge ein:

1. Halten Sie die umschalttaste und entweder die Taste strg oder alt (oder eine andere festgelegte Kombination) gedrückt, während Sie die Taste für das ausgewählte Zeichen drücken.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Verwenden des File Sanitizer-Symbols

ACHTUNG: Geshredderte Datenbestände können nicht wiederhergestellt werden. Gehen Sie daher bei der Auswahl von Datenbeständen für manuelles Shreddern mit Bedacht vor.

1. Navigieren Sie zu dem Dokument oder Ordner, das bzw. der geshreddert werden soll.
2. Ziehen Sie den Datenbestand auf das **File Sanitizer**-Symbol auf dem Desktop.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Shreddern von Datenbeständen

ACHTUNG: Geshredderte Datenbestände können nicht wiederhergestellt werden. Gehen Sie daher bei der Auswahl von Datenbeständen für manuelles Shreddern mit Bedacht vor.

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Ein Element shreddern**.
2. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.

   HINWEIS: Bei dem von Ihnen ausgewählten Datenbestand kann es sich um eine einzelne Datei oder einen einzelnen Ordner handeln.

3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Desktop, und klicken Sie dann auf **Ein Element shreddern**.
2. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Klicken Sie auf die Schaltfläche **Durchsuchen**.
3. Navigieren Sie nach dem Öffnen des Dialogfelds **Durchsuchen** zu dem Datenbestand, den Sie shreddern möchten, und klicken Sie anschließend auf **OK**.
4. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Shreddern aller ausgewählter Elemente

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Klicken Sie mit der rechten Maustaste auf das Symbol **File Sanitizer** auf dem Desktop, und klicken Sie dann auf **Jetzt shreddern**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Shreddern**.
2. Klicken Sie auf die Schaltfläche **Jetzt shreddern**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Manuelles Aktivieren des Überschreibens von freiem Speicherplatz

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools** im Infobereich der Taskleiste (rechts außen). Klicken Sie auf **File Sanitizer** und anschließend auf **Jetzt überschreiben**.
2. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

– ODER –

1. Öffnen Sie File Sanitizer, und klicken Sie auf **Festplattenbereinigung**.
2. Klicken Sie auf **Jetzt überschreiben**.
3. Klicken Sie im daraufhin erscheinenden Bestätigungsdialogfeld auf **Ja**.

Abbrechen eines Shred- oder Überschreibungsvorgangs

Während eines Shred- oder Überschreibungsvorgangs wird über dem Symbol von HP ProtectTools Security Manager im Infobereich ganz rechts in der Taskleiste eine entsprechende Meldung angezeigt. Sie enthält Details zum laufenden Vorgang (Prozentsatz der Fertigstellung) sowie eine Option zum Abbrechen des Shred-/Überschreibungsvorgangs.

▲ Zum Abbrechen des Vorgangs klicken Sie auf die Meldung und anschließend auf **Stopp**.

Anzeigen der Protokolldateien

Für jeden Shred-Vorgang und jedes Überschreiben von freiem Speicherplatz werden Protokolldateien erzeugt, die eventuell während der Ausführung aufgetretene Fehler aufzeichnen. Die Protokolldateien werden immer wieder aktualisiert, sodass sich ihr Inhalt jeweils auf den letzten Shred-Vorgang bzw. die letzte Überschreibung bezieht.

HINWEIS: Dateien, die erfolgreich geshreddert wurden, oder erfolgreiche Überschreibevorgänge werden in den Protokolldateien nicht aufgeführt.

Das System erzeugt eine Protokolldatei für Shred- und eine für Überschreibungsvorgänge. Beide Protokolldateien befinden sich auf der Festplatte in folgenden Verzeichnissen:

- C:\Programme\Hewlett-Packard\File Sanitizer*[Benutzername]*_ShredderLog.txt
- C:\Programme\Hewlett-Packard\File Sanitizer*[Benutzername]*_DiskBleachLog.txt

Bei 64-Bit-Systemen sind die Protokolldateien auf der Festplatte in diesen Verzeichnissen abgelegt:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Benutzername]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Benutzername]*_DiskBleachLog.txt

8 Device Access Manager for HP ProtectTools (bestimmte Modelle)

Mithilfe von HP ProtectTools Device Access Manager kann der Datenzugriff gesteuert werden, indem Datenübertragungsgeräte deaktiviert werden.

HINWEIS: Einige Schnittstellen/Eingabegeräte für die Benutzerinteraktion, wie Maus, Tastatur, TouchPad und Fingerabdruck-Lesegeräte, können nicht über Device Access Manager gesteuert werden. Weitere Informationen finden Sie unter „Nicht verwaltete Geräteklassen“ auf Seite 102.

Windows® Administratoren verwenden HP ProtectTools Device Access Manager, um den Zugriff auf die Geräte eines Systems zu steuern und einen unbefugten Zugriff zu verhindern:

- Für jeden Benutzer werden Geräteprofile erstellt. Diese definieren, auf welche Geräte der Benutzer Zugriff bzw. keinen Zugriff hat.
- Mittels Just-In-Time-Authentifizierung (JITA) können sich vordefinierte Benutzer authentifizieren, um Zugriff auf Geräte zu erhalten, die normalerweise gesperrt sind.
- Administratoren und vertrauenswürdige Benutzer können aus den Beschränkungen für den Gerätezugriff durch Device Access Manager ausgenommen werden, indem sie zur Gruppe „Geräte-Administratoren“ hinzugefügt werden. Die Mitgliedschaft in dieser Gruppe wird über „Erweiterte Einstellungen“ verwaltet.
- Der Gerätezugriff kann auf der Grundlage der Gruppenzugehörigkeit bzw. für einzelne Benutzer erteilt oder verweigert werden.
- Für Geräteklassen, wie z. B. CD-ROM- und DVD-Laufwerke, können unterschiedliche Rechte für Lese- und Schreibzugriff erteilt werden.

Öffnen von Device Access Manager

1. Melden Sie sich als Administrator an.
2. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
3. Klicken Sie im linken Fensterausschnitt auf **Device Access Manager**.

Benutzer mit eingeschränkten Rechten können die HP ProtectTools Device Access Manager Richtlinie mit HP ProtectTools Security Manager anzeigen. Mit dieser Konsole ist nur eine schreibgeschützte Ansicht möglich.

Setup-Verfahren

Konfigurieren von Zugriffrechten auf Geräte

In HP ProtectTools Device Access Manager sind vier Ansichten verfügbar:

- **Einfache Konfiguration**: Erteilen oder verweigern Sie den Zugriff auf Geräteklassen auf der Grundlage der Mitgliedschaft in der Gruppe „Geräte-Administratoren“.
- **Geräteklassen-Konfiguration**: Erteilen oder verweigern Sie den Zugriff auf Gerätetypen oder bestimmte Geräte für bestimmte Benutzer oder Gruppen.
- **JITA-Konfiguration**: Konfigurieren Sie eine Just-In-Time-Authentifizierung (JITA), um ausgewählten Benutzern den Zugriff auf DVD-/CD-ROM-Laufwerke oder Wechselmedien zu erlauben, wenn sie sich authentifizieren.
- **Erweiterte Einstellungen**: Konfigurieren Sie eine Liste mit Laufwerksbuchstaben, für die der Zugriff durch Device Access Manager nicht beschränkt ist, wie beispielsweise das Laufwerk C (Systemlaufwerk). In dieser Ansicht kann außerdem die Mitgliedschaft in der Gruppe „Geräte-Administratoren“ verwaltet werden.

Einfache Konfiguration

Administratoren können die Ansicht **Einfache Konfiguration** verwenden, um den Zugriff auf die folgenden Geräteklassen für alle Benutzer, die keine Geräte-Administratoren sind, zu erteilen oder zu verweigern:

- Alle Wechselmedien (Disketten, USB-Flash-Laufwerke usw.)
- Alle DVD-/CD-ROM-Laufwerke
- Alle seriellen und parallelen Anschlüsse
- Alle Bluetooth®-Geräte
- Alle Modems
- Alle PCMCIA-/ExpressCard-Geräte
- Alle 1394-Geräte

So erteilen oder verweigern Sie allen Benutzern, die keine Geräte-Administratoren sind, den Zugriff auf eine Geräteklasse:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Einfache Konfiguration**.
2. Um den Zugriff zu verweigern, aktivieren Sie im rechten Fensterausschnitt das Kontrollkästchen für eine Geräteklasse oder ein bestimmtes Gerät. Deaktivieren Sie das Kontrollkästchen, um den Zugriff auf die Geräteklasse oder das Gerät zu erteilen.

   Wenn ein Kontrollkästchen abgeblendet dargestellt wird, wurden die Werte, die sich auf das Zugriffsszenario auswirken, innerhalb der Ansicht **Geräteklassen-Konfiguration** geändert. Klicken Sie zum Wiederherstellen der Werkseinstellungen in der Ansicht **Geräteklassen-Konfiguration** auf **Zurücksetzen**.
3. Klicken Sie auf **Übernehmen**.

HINWEIS: Wenn der Hintergrunddienst nicht aktiv ist, werden Sie gefragt, ob Sie den Dienst starten möchten. Klicken Sie auf **Ja**.

4. Klicken Sie auf **OK**.

Starten des Hintergrunddienstes

Wenn das erste Mal eine neue Richtlinie festgelegt und angewendet wird, startet der Hintergrunddienst HP ProtectTools Gerätesperre/Überwachung automatisch und ist so eingestellt, dass er bei jedem Systemstart automatisch startet.

HINWEIS: Bevor die Eingabeaufforderung für den Hintergrunddienst angezeigt wird, muss ein Geräteprofil definiert werden.

Administratoren können diesen Dienst auch starten oder stoppen:

1. Klicken Sie unter Windows 7 auf **Start**, **Systemsteuerung** und anschließend auf **System und Sicherheit**.

   – oder –

   Klicken Sie unter Windows Vista® auf **Start**, **Systemsteuerung** und anschließend auf **System und Wartung**.

   – oder –

   Klicken Sie unter Windows XP auf **Start**, **Systemsteuerung** und anschließend auf **Leistung und Wartung**.

2. Klicken Sie auf **Verwaltung** und dann auf **Dienste**.

3. Wählen Sie den Dienst **HP ProtectTools Gerätesperre/Überwachung**.

4. Klicken Sie zum Starten des Diensts auf **Start**.

   – oder –

   Klicken Sie zum Stoppen des ausgeführten Diensts auf **Stopp**.

Wenn Sie den Dienst „Gerätesperre/Überwachung“ stoppen, bleibt die Gerätesperre erhalten. Die Gerätesperre wird durch zwei Komponenten in Kraft gesetzt:

- Den Dienst „Gerätesperre/Überwachung“
- Den Treiber DAMDrv.sys

Wenn Sie den Dienst starten, wird auch der Gerätetreiber gestartet. Der Treiber wird jedoch nicht gestoppt, wenn Sie den Dienst stoppen.

Um festzustellen, ob der Hintergrunddienst aktiv ist, öffnen Sie ein Eingabeaufforderungsfenster, und geben Sie `sc query flcdlock` ein.

Um festzustellen, ob der Gerätetreiber aktiv ist, öffnen Sie ein Eingabeaufforderungsfenster, und geben Sie `sc query damdrv` ein.

Geräteklassen-Konfiguration

Administratoren können Listen mit Benutzern und Gruppen, die Zugriff bzw. keinen Zugriff auf Geräteklassen oder bestimmte Geräte haben, anzeigen und ändern.

Die Ansicht **Geräteklassen-Konfiguration** besteht aus den folgenden Bereichen:

- **Geräteliste** – Zeigt alle Geräteklassen und Geräte an, die auf dem System installiert sind oder bereits auf dem System installiert waren.
  - In der Regel erstreckt sich der Schutz auf eine Geräteklasse. Ein ausgewählter Benutzer oder eine ausgewählte Gruppe kann auf alle Geräte der Geräteklasse zugreifen.
  - Es besteht außerdem die Möglichkeit, bestimmte Geräte zu schützen.
- **Benutzerliste** – Zeigt alle Benutzer und Gruppen an, denen Zugriff auf die gewählte Geräteklasse bzw. ein bestimmtes Gerät gewährt oder verweigert wurde.
  - Der Eintrag in der Benutzerliste kann sich auf einen bestimmten Benutzer oder auf eine Gruppe beziehen, zu der der Benutzer gehört.
  - Wenn ein Benutzer- oder Gruppeneintrag in der Benutzerliste nicht verfügbar ist, wurden die Einstellungen übernommen, die für die Geräteklasse in der Geräteliste oder im Ordner „Klassen“ festgelegt wurden.
  - Der Zugriff auf einige Geräteklassen (z. B. DVD- und CD-ROM-Laufwerke) kann auch gesteuert werden, indem unterschiedliche Rechte für Lese- und Schreibzugriff erteilt werden.

    Für andere Geräte und Klassen können die Rechte für Lese- und Schreibzugriff übernommen werden. Beispielsweise kann der Lesezugriff von einer höheren Klasse übernommen werden, aber der Schreibzugriff kann speziell für einen Benutzer oder eine Gruppe verweigert werden.

    HINWEIS: Ein deaktiviertes Kontrollkästchen **Lesen** bedeutet, dass der Eintrag für die Zugriffssteuerung keine Auswirkung auf den Lesezugriff auf das Gerät hat. Der Lesezugriff wird jedoch nicht verweigert.

    HINWEIS: Die Gruppe „Administratoren“ kann nicht zur „Benutzerliste“ hinzugefügt werden. Verwenden Sie stattdessen die Gruppe „Geräte-Administratoren“.

    Beispiel 1 – Einem Benutzer oder einer Gruppe wird Schreibzugriff auf ein Gerät oder eine Geräteklasse verweigert:

    Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Schreib- oder Lese-/Schreibzugriff für ein Gerät erteilt werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

    Beispiel 2 – Einem Benutzer oder einer Gruppe wird Schreibzugriff auf ein Gerät oder eine Geräteklasse gewährt:

    Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Schreib- oder Lese-/Schreibzugriff für das Gerät selbst oder ein Gerät verweigert werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

    Beispiel 3 – Einem Benutzer oder einer Gruppe wird Lesezugriff auf ein Gerät oder eine Geräteklasse gewährt:

    Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Lese- oder Lese-/Schreibzugriff für das Gerät selbst oder ein Gerät verweigert werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

    Beispiel 4 – Einem Benutzer oder einer Gruppe wird Lesezugriff auf ein Gerät oder eine Geräteklasse verweigert:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Lese- oder Lese-/Schreibzugriff für ein Gerät erteilt werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 5 – Einem Benutzer oder einer Gruppe wird Lese-/Schreibzugriff auf ein Gerät oder eine Geräteklasse gewährt:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Schreib- oder Lese-/Schreibzugriff für das Gerät selbst oder ein Gerät verweigert werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Beispiel 6 – Einem Benutzer oder einer Gruppe wird Lese-/Schreibzugriff auf ein Gerät oder eine Geräteklasse verweigert:

Dem Benutzer, der Gruppe oder einem Mitglied der Gruppe kann nur Lese- oder Lese-/Schreibzugriff für ein Gerät erteilt werden, das sich in der Gerätehierarchie unter dem Gerät befindet.

Zugriff für Benutzer oder Gruppe verweigern

Gehen Sie folgendermaßen vor, um einem Benutzer oder einer Gruppe den Zugriff auf ein Gerät oder eine Geräteklasse zu verwehren:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll.
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Wählen Sie unter **Benutzer/Gruppen** den Benutzer bzw. die Gruppe aus, der/die keinen Zugriff erhalten soll, und klicken Sie dann auf **Verweigern**.
4. Klicken Sie auf **Übernehmen**.

HINWEIS: Wenn für einen Benutzer auf derselben Geräteebene Zugriff verweigert und erteilt wird, hat die Zugriffsverweigerung Vorrang.

Zugriff für Benutzer oder Gruppe erteilen

So erteilen Sie einem Benutzer oder einer Gruppe Zugriff auf ein Gerät oder eine Geräteklasse:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf eines der folgenden Elemente:
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.

4. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach Benutzern und Gruppen zu suchen, die hinzugefügt werden sollen.
5. Klicken Sie auf einen Benutzer oder eine Gruppe, der bzw. die zur Liste der verfügbaren Benutzer und Gruppen hinzugefügt werden soll, und klicken Sie anschließend auf **OK**.
6. Klicken Sie erneut auf **OK**.
7. Klicken Sie auf **Zulassen**, um diesem Benutzer Zugriff zu gewähren.
8. Klicken Sie auf **Übernehmen**.

Einem Benutzer einer Gruppe Zugriff auf eine Geräteklasse erteilen

Gehen Sie folgendermaßen vor, um einem Benutzer Zugriff auf eine Gerätklasse zu erteilen, während Sie allen anderen Mitgliedern der Gruppe den Zugriff verweigern:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll.
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Wählen Sie unter **Benutzer/Gruppen** die Gruppe aus, die keinen Zugriff erhalten soll, und klicken Sie dann auf **Verweigern**.
4. Navigieren Sie zu dem Ordner unter dem der erforderlichen Klasse, und fügen Sie den entsprechenden Benutzer hinzu.
5. Klicken Sie auf **Zulassen**, um diesem Benutzer Zugriff zu gewähren.
6. Klicken Sie auf **Übernehmen**.

Einem Benutzer einer Gruppe Zugriff auf ein bestimmtes Gerät erteilen

Administratoren können einem Benutzer den Zugriff auf ein bestimmtes Gerät gewähren, während sie allen anderen Mitgliedern der Gruppe den Zugriff auf alle Geräte verweigern, die in der Klasse enthalten sind:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll, und navigieren Sie zu dem Ordner darunter.
3. Klicken Sie unter **Benutzer/Gruppen** neben der Gruppe, die Zugriff erhalten soll, auf **Zulassen**.
4. Klicken Sie neben der Gruppe, die keinen Zugriff erhalten soll, auf **Verweigern**.
5. Navigieren Sie in der Geräteliste zu dem Gerät, auf das der Benutzer Zugriff erhalten soll.
6. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Benutzer oder Gruppen auswählen** wird geöffnet.
7. Klicken Sie auf **Erweitert** und dann auf **Jetzt suchen**, um nach Benutzern und Gruppen zu suchen, die hinzugefügt werden sollen.
8. Klicken Sie auf einen Benutzer, der Zugriff erhalten soll, und dann auf **OK**.
9. Klicken Sie auf **Zulassen**, um diesem Benutzer Zugriff zu gewähren.
10. Klicken Sie auf **Übernehmen**.

Entfernen von Einstellungen für einen Benutzer oder eine Gruppe

So entziehen Sie einem Benutzer oder einer Gruppe die Zugriffsberechtigung für ein Gerät oder eine Geräteklasse:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie in der Geräteliste auf die Geräteklasse, die konfiguriert werden soll.
   - **Geräteklasse**
   - **Alle Geräte**
   - **Einzelnes Gerät**
3. Klicken Sie unter **Benutzer/Gruppen** auf den Benutzer bzw. die Gruppe, der bzw. die entfernt werden soll, und klicken anschließend auf **Entfernen**.
4. Klicken Sie auf **Übernehmen**.

Zurücksetzen der Konfiguration

ACHTUNG: Beim Zurücksetzen der Konfiguration werden alle Änderungen an der Gerätekonfiguration verworfen, und alle Werkseinstellungen werden wiederhergestellt.

So setzen Sie die Konfigurationseinstellungen auf die Werkseinstellungen zurück:

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **Geräteklassen-Konfiguration**.
2. Klicken Sie auf **Zurücksetzen**.
3. Klicken Sie in der Bestätigungsaufforderung auf **Ja**.
4. Klicken Sie auf **Übernehmen**.

JITA-Konfiguration

Mithilfe der JITA-Konfiguration kann der Administrator Listen mit Benutzern und Gruppen anzeigen und bearbeiten, die unter Verwendung der Just-In-Time-Authentifizierung (JITA) auf Geräte zugreifen dürfen.

JITA-aktivierte Benutzer können auf einige Geräte zugreifen, für die in der Ansicht **Geräteklassen-Konfiguration** oder **Einfache Konfiguration** erstellte Richtlinien beschränkt wurden.

- **Szenario** – Eine Richtlinie für eine einfache Konfiguration wird konfiguriert, um allen Benutzern, die keine Geräte-Administratoren sind, Zugriff auf das DVD-/CD-ROM-Laufwerk zu verweigern.
- **Ergebnis** – Ein JITA-aktivierter Benutzer, der auf das DVD-/CD-ROM-Laufwerk zugreifen möchte, erhält dieselbe Meldung aufgrund verweigerten Zugriffs wie ein Benutzer, der nicht für JITA aktiviert ist. Anschließend wird eine Ballon-Nachricht angezeigt, mit der Frage, ob der Benutzer JITA-Zugriff möchte. Wenn der Benutzer auf den Ballon klickt, wird das Dialogfeld für die Benutzerauthentifizierung geöffnet. Gibt der Benutzer seine Anmeldeinformationen erfolgreich ein, wird der Zugriff auf das DVD-/CD-ROM-Laufwerk erteilt.

Der JITA-Zeitraum kann für eine festgelegte Anzahl an Minuten oder 0 Minuten genehmigt sein. Ein JITA-Zeitraum von 0 Minuten kann nicht ablaufen. Benutzer können ab dem Zeitpunkt der Authentifizierung bis zur Abmeldung vom System auf das Gerät zugreifen.

Der JITA-Zeitraum kann bei entsprechender Konfiguration auch verlängert werden. In diesem Szenario können Benutzer 1 Minute vor Ablauf des JITA-Zeitraums auf die Aufforderung klicken, um ihren Zugriff ohne erneute Authentifizierung zu verlängern.

Unabhängig davon, ob der Benutzer einen beschränkten oder unbeschränkten JITA-Zeitraum zur Verfügung hat, läuft der JITA-Zeitraum ab, wenn sich der Benutzer vom System abmeldet bzw. sich ein anderer Benutzer anmeldet. Wenn der Benutzer sich das nächste Mal anmeldet und versucht, auf ein JITA-aktiviertes Gerät zuzugreifen, wird eine Aufforderung zur Eingabe der Anmeldeinformationen angezeigt.

JITA ist für die folgenden Geräteklassen verfügbar:

- DVD-/CD-ROM-Laufwerke
- Wechselmedien

Erstellen einer JITA für einen Benutzer oder eine Gruppe

Administratoren können Benutzern oder Gruppen Zugriff auf Geräte mit der Just-In-Time-Authentifizierung erteilen.

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **JITA-Konfiguration**.
2. Wählen Sie im Dropdown-Menü des Geräts entweder **Wechselmedien** oder **DVD/CD-ROM-Laufwerke**.
3. Klicken Sie auf **+**, um einen Benutzer oder eine Gruppe zur JITA-Konfiguration hinzuzufügen.
4. Wählen Sie das Kontrollkästchen **Aktiviert** aus.
5. Legen Sie den JITA-Zeitraum auf den gewünschten Wert fest.
6. Klicken Sie auf **Übernehmen**.

Der Benutzer muss sich abmelden und erneut anmelden, damit die neue JITA-Einstellung übernommen wird.

Erstellen einer verlängerbaren JITA für einen Benutzer oder eine Gruppe

Administratoren können einen Benutzer- oder Gruppenzugriff auf Geräte mit Just-In-Time-Authentifizierung erteilen, die der Benutzer verlängern kann, bevor sie abläuft.

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **JITA-Konfiguration**.
2. Wählen Sie im Dropdown-Menü des Geräts entweder **Wechselmedien** oder **DVD/CD-ROM-Laufwerke**.
3. Klicken Sie auf **+**, um einen Benutzer oder eine Gruppe zur JITA-Konfiguration hinzuzufügen.
4. Wählen Sie das Kontrollkästchen **Aktiviert** aus.
5. Legen Sie den JITA-Zeitraum auf den gewünschten Wert fest.
6. Wählen Sie das Kontrollkästchen **Verlängerbar** aus.
7. Klicken Sie auf **Übernehmen**.

Der Benutzer muss sich abmelden und erneut anmelden, damit die neue JITA-Einstellung übernommen wird.

Deaktivieren einer JITA für einen Benutzer oder eine Gruppe

Administratoren können den Zugriff von Benutzern oder Gruppen auf Geräte mit der Just-In-Time-Authentifizierung deaktivieren.

1. Klicken Sie im linken Fensterausschnitt von HP ProtectTools Administrator-Konsole auf **Device Access Manager** und anschließend auf **JITA-Konfiguration**.
2. Wählen Sie im Dropdown-Menü des Geräts entweder **Wechselmedien** oder **DVD/CD-ROM-Laufwerke**.
3. Wählen Sie den Benutzer oder die Gruppe, für den/die JITA deaktiviert werden soll.

4. Deaktivieren Sie das Kontrollkästchen **Aktiviert**.
5. Klicken Sie auf **Übernehmen**.

Wenn sich der Benutzer anmeldet und versucht, auf das Gerät zuzugreifen, wird der Zugriff verweigert.

Erweiterte Einstellungen

Mit „Erweiterte Einstellungen“ stehen Ihnen die folgenden Funktionen zur Verfügung:

- Verwaltung der Gruppe „Geräte-Administratoren“
- Verwaltung von Laufwerksbuchstaben, für die Device Access Manager nie den Zugriff verweigert

Die Gruppe „Geräte-Administratoren“ wird verwendet, um vertrauenswürdige Benutzer (vertrauenswürdig im Hinblick auf den Gerätezugriff) von den Beschränkungen durch eine Device Access Manager Richtlinie auszunehmen. Systemadministratoren gehören üblicherweise zu den vertrauenswürdigen Benutzern. Weitere Informationen finden Sie unter „Gruppe „Geräte-Administratoren““ auf Seite 101.

In der Ansicht **Erweiterte Einstellungen** kann der Administrator zudem eine Liste mit Laufwerksbuchstaben konfigurieren, für die Device Access Manager den Zugriff für Benutzer nicht beschränkt.

HINWEIS: Die Hintergrunddienste für Device Access Manager müssen ausgeführt werden, wenn die Liste mit den Laufwerksbuchstaben konfiguriert wird.

So starten Sie diese Dienste:

1. Wenden Sie eine Richtlinie für eine einfache Konfiguration an, wie beispielsweise die Zugriffsverweigerung auf Wechselmedien für alle Benutzer, die keine Geräte-Administratoren sind.

   – oder –

   Öffnen Sie mit Administratorrechten ein Eingabeaufforderungsfenster, und geben Sie Folgendes ein:

   ```
   sc start flcdlock
   ```

   Drücken Sie die Eingabetaste.

2. Sobald die Dienste gestartet wurden, kann die Laufwerksliste bearbeitet werden. Geben Sie die Laufwerksbuchstaben von Geräten ein, die nicht von Device Access Manager gesteuert werden sollen.

   Die Laufwerksbuchstaben werden für physische Festplatten oder Partitionen angezeigt.

   HINWEIS: Unabhängig davon, ob sich das Systemlaufwerk (üblicherweise C) in der Liste befindet, wird der Zugriff darauf nie für Benutzer verweigert.

Gruppe „Geräte-Administratoren“

Bei der Installation von Device Access Manager wird die Gruppe „Geräte-Administratoren” erstellt.

Die Gruppe „Geräte-Administratoren“ wird verwendet, um vertrauenswürdige Benutzer (vertrauenswürdig im Hinblick auf den Gerätezugriff) von den Beschränkungen durch eine Device Access Manager Richtlinie auszunehmen. Systemadministratoren gehören üblicherweise zu den vertrauenswürdigen Benutzern.

HINWEIS: Die Aufnahme eines Benutzers in die Gruppe „Geräte-Administratoren“ berechtigt ihn nicht automatisch zum Gerätezugriff. Wenn der Gruppe „Benutzer“ in der Ansicht **Geräteklassen-Konfiguration** der Zugriff auf ein Gerät verweigert wird, muss der Gruppe „Geräte-Administratoren“ der Zugriff erlaubt werden, damit Mitglieder der Gruppe Zugriff auf das Gerät haben. Die Ansicht **Einfache Konfiguration** kann jedoch verwendet werden, um allen Benutzern, die kein Mitglied der Gruppe „Geräte-Administratoren“ sind, den Zugriff auf Geräteklassen zu verweigern.

So fügen Sie Benutzer zur Gruppe „Geräte-Administratoren“ hinzu:

1. Klicken Sie in der Ansicht **Erweiterte Einstellungen** auf **+**.
2. Geben Sie den Benutzernamen des vertrauenswürdigen Benutzers ein.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf **Übernehmen**.

Alternative Methoden zum Verwalten der Mitgliedschaft in dieser Gruppe sind u. a.:

- Unter Windows 7 Professional oder Windows Vista können Benutzer über das Standard-Snap-In von Microsoft Management Console (MMC) „Lokale Benutzer und Gruppen“ zu dieser Gruppe hinzugefügt werden.
- Für die Home-Versionen von Windows 7, Windows Vista oder Windows XP geben Sie den folgenden Befehl über ein Administratorkonto in ein Eingabeaufforderungsfenster ein:

  ```
  net localgroup "Geräte-Administratoren" benutzername /Add
  ```

  In diesem Befehl ist „benutzername“ der Benutzername des Benutzers, der zu dieser Gruppe hinzugefügt werden soll.

eSATA-Support

Damit Device Access Manager eSATA-Geräte steuern kann, muss Folgendes konfiguriert werden:

1. Das Laufwerk muss verbunden werden, wenn das System startet.
2. Stellen Sie über die Ansicht **Erweiterte Einstellungen** sicher, dass der Buchstabe des eSATA-Laufwerks nicht in der Liste der Laufwerke enthalten ist, für die Device Access Manager den Zugriff nicht verweigert. Wenn der Buchstabe des eSATA-Laufwerks aufgeführt ist, löschen Sie den Laufwerksbuchstaben, und klicken Sie dann auf **Übernehmen**.
3. Das Gerät kann über die Ansicht **Einfache Konfiguration** oder **Geräteklassen-Konfiguration** anhand der Geräteklasse „Wechselmedien“ gesteuert werden.

Nicht verwaltete Geräteklassen

HP ProtectTools Device Access Manager verwaltet die folgenden Geräteklassen nicht:

- Eingabe-/Ausgabegeräte
  - Biometrisches Gerät
  - Maus
  - Tastatur
  - Drucker

- Plug-and-Play (PnP)-Drucker
- Drucker-Upgrade
- Infrarot-Schnittstelle für die Benutzerinteraktion
- Lesegerät für Smart Cards
- Serieller Multi-Port
- Datenträgerlaufwerk
- Disketten-Controller (FDC)
- Festplatten-Controller (HDC)
- Schnittstelle für die Benutzerinteraktion (HID)

- Energie
  - Akku
  - Support für erweiterte Energieverwaltung (APM)
- Sonstiges
  - Computer
  - Decoder
  - Display
  - Prozessor
  - System
  - Unbekannt
  - Lautstärke
  - Volume-Schnappschuss
  - Sicherheitsgerät
  - Sicherheitsbeschleuniger
  - Vereinheitlichter Anzeigetreiber von Intel®
  - Medientreiber
  - Medienwechselgerät
  - Multifunktionsgerät
  - Legacard
  - Netz-Client
  - Netzdienst

- Netzübertragung
- SCSI-Adapter

9 Wiederbeschaffung gestohlener Geräte

Mit Computrace for HP ProtectTools (separat erhältlich) können Sie Ihren Computer per Fernzugriff überwachen, verwalten und wiederfinden.

Nach der Aktivierung wird Computrace for HP ProtectTools vom Absolute Software-Kundencenter konfiguriert. Vom Kundencenter aus kann der Administrator Computrace for HP ProtectTools konfigurieren, um den Computer zu überwachen oder zu verwalten. Wenn der Computer verloren geht oder gestohlen wird, kann das Kundencenter die lokalen Behörden bem Auffinden und bei der Wiederbeschaffung des Computers unterstützen. Nach der Konfiguration bleibt Computrace auf dem Computer auch dann aktiv, wenn die Festplatte gelöscht oder ausgetauscht wird.

So aktivieren Sie Computrace for HP ProtectTools:

1. Stellen Sie eine Verbindung zum Internet her.
2. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
3. Klicken Sie auf der linken Seite von Security Manager auf **Theft Recovery** (Wiedererlangen bei Diebstahl).
4. Zum Starten des Computrace Aktivierungsassistenten klicken Sie auf die Schaltfläche **Activate Now** (Jetzt aktivieren).
5. Geben Sie Ihre Kontakt- und Kreditkarteninformationen oder einen bereits gekauften Produktschlüssel ein.

Der Aktivierungsassistent verarbeitet die Transaktion auf sichere Weise und richtet Ihr Benutzerkonto auf der Website des Absolute Software-Kundencenters ein. Anschließend erhalten Sie eine Bestätigungs-E-Mail mit den Informationen zu Ihrem Kundencenter-Konto.

Wenn Sie den Computrace Aktivierungsassistenten schon einmal ausgeführt haben und bereits über ein Kundencenter-Benutzerkonto verfügen, können Sie zusätzliche Lizenzen erwerben. Weitere Informationen erhalten Sie von Ihrem HP Kundenberater.

So melden Sie sich beim Kundencenter an:

1. Rufen Sie folgende Adresse auf: https://cc.absolute.com/.
2. Geben Sie in die Felder **Benutzername** und **Kennwort** die Informationen ein, die Sie in der Bestätigungs-E-Mail erhalten haben, und klicken Sie auf die Schaltfläche **Anmelden**.

Im Kundencenter können Sie:

- Ihre Computer überwachen.
- Ihre Remote-Daten schützen.
- Den Diebstahl von Computern melden, die durch Computrace geschützt sind.

▲ Klicken Sie auf **Weitere Informationen**, um zusätzliche Informationen über Computrace for HP ProtectTools zu erhalten.

10 Embedded Security for HP ProtectTools (bestimmte Modelle)

HINWEIS: Der TPM-Chip (Trusted Platform Module) für integrierte Sicherheit muss im Computer installiert sein, um Embedded Security for HP ProtectTools zu verwenden.

Embedded Security for HP ProtectTools schützt vor unberechtigtem Zugriff auf Benutzerdaten oder Berechtigungen. Dieses Softwaremodul enthält folgende Sicherheitsfunktionen:

- Enhanced Microsoft® Encryption File System (EFS)-Datei und Ordnerverschlüsselung
- Erstellen eines PSD (Personal Secure Drive, Persönliches Sicherheitslaufwerk) zum Schutz der Benutzerdaten
- Datenverwaltungsfunktionen, wie Sichern und Wiederherstellen der Haupthierarchie
- Unterstützung für Anwendungen von Fremdherstellern (wie Microsoft Outlook und Internet Explorer) für geschützte digitale Zertifikatoperationen bei der Verwendung der Embedded Security Software

Die integrierte TPM-Sicherheitschip aktiviert und unterstützt weitere Sicherheitsfunktionen von HP ProtectTools Security Manager. Zum Beispiel kann Credential Manager for HP ProtectTools den integrierten Chip als Authentifizierungsfaktor verwenden, wenn sich der Benutzer bei Windows anmeldet.

Setup-Verfahren

⚠ **ACHTUNG:** Um Sicherheitsrisiken zu vermeiden, wird empfohlen, dass der IT-Administrator den integrierten Sicherheitschip sofort initialisiert. Geschieht dies nicht, so kann ein nicht autorisierter Benutzer, ein Computerwurm oder ein Virus die Steuerung des Computers und der Eigentümertasks übernehmen, wie zum Beispiel die Verwendung des Notfall-Wiederherstellungsarchivs und die Konfiguration von Benutzerzugriffseinstellungen.

Befolgen Sie die Schritte in den folgenden Absätzen, um den integrierten Sicherheitschip zu aktivieren und zu initialisieren.

Aktivieren des integrierten Sicherheitschips in Computer Setup

Der integrierte Sicherheitschip muss im Schnell-Initialisierungsassistenten oder mit dem Computer Setup Utility aktiviert werden.

So aktivieren Sie den integrierten Sicherheitschip in Computer Setup:

1. Öffnen Sie Computer Setup, indem Sie den Computer einschalten oder neu starten und die Taste f10 drücken, während die Meldung „f10 = ROM Based Setup“ (f10 = ROM-basiertes Setup) unten links auf dem Bildschirm angezeigt wird.
2. Wenn Sie noch kein Administratorkennwort eingerichtet haben, wählen Sie mit den Pfeiltasten die Option **Security** (Sicherheit) und dann **Setup password** (Kennwort einrichten) aus, und drücken Sie die Eingabetaste.
3. Geben Sie ein Kennwort in die Felder **New password** (Neues Kennwort) und **Verify new password** (Neues Kennwort bestätigen) ein, und drücken Sie anschließend f10.
4. Wählen Sie im Menü **Security** (Sicherheit) mit den Pfeiltasten **TPM Embedded Security** aus, und drücken Sie die Eingabetaste.
5. Wählen Sie unter **Embedded Security** die Option **Available** (Verfügbar) aus, wenn das Gerät ausgeblendet ist.
6. Wählen Sie **Embedded security device state** (Status des integrierten Sicherheitsgeräts) aus, und ändern Sie die Einstellung auf **Enable** (Aktivieren).
7. Drücken Sie f10, um die Änderungen an der Embedded Security-Konfiguration zu akzeptieren.
8. Um Ihre Einstellungen zu speichern und Computer Setup zu verlassen, wählen Sie mit den Pfeiltasten **File** (Datei) und dann **Save Changes and Exit** (Änderungen speichern und beenden) aus und folgen anschließend den Anleitungen auf dem Bildschirm.

Initialisieren des integrierten Sicherheitschips

Während des Initialisierungsvorgangs für Embedded Security führen Sie Folgendes aus:

- Richten Sie ein Eigentümerkennwort für den Chip für integrierte Sicherheit ein, um den Zugriff auf alle Eigentümerfunktionen auf dem Chip für integrierte Sicherheit zu schützen.
- Richten Sie das Archiv für die Notfallwiederherstellung ein. Hierbei handelt es sich um einen geschützten Speicherbereich, der die erneute Verschlüsselung der allgemeinen Benutzerschlüssel für alle Benutzer ermöglicht.

So initialisieren Sie den Chip für integrierte Sicherheit:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **HP ProtectTools Security Manager** im Infobereich der Taskleiste (rechts außen). Wählen Sie dann **Embedded Security Initialization** (Initialisierung von Embedded Security) aus.

   Der Assistent für die Initialisierung der HP ProtectTools Embedded Security wird geöffnet.

2. Folgen Sie den Anleitungen auf dem Bildschirm.

Einrichten eines einfachen Benutzerkontos

Die Einrichtung eines allgemeinen Benutzerkontos in Embedded Security führt Folgendes aus:

- Erstellt einen allgemeinen Benutzerschlüssel, der die verschlüsselten Informationen schützt, und richtet ein Kennwort für den allgemeinen Benutzerschlüssel ein, um diesen zu schützen.
- Richtet ein PSD (Personal Secure Drive, persönliches Sicherheitslaufwerk) zum Speichern verschlüsselter Dateien und Ordner ein.

ACHTUNG: Bewahren Sie das Kennwort für den allgemeinen Benutzerschlüssel sorgfältig auf. Der Zugriff auf oder die Wiederherstellung von verschlüsselten Informationen ist ohne dieses Kennwort nicht möglich.

So richten Sie ein allgemeines Benutzerkonto ein und aktivieren die Sicherheitsfunktionen für den Benutzer:

1. Wenn der Initialisierungsassistent von Embedded Security nicht geöffnet ist, klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterausschnitt unter **Embedded Security Features** (Embedded Security-Funktionen) auf **Konfigurieren**.

   Der Assistent für die Benutzerinitialisierung der Embedded Security wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

   HINWEIS: Um die Funktionalität sicherer E-Mails verwenden zu können, müssen Sie zunächst Ihr E-Mail-Programm so konfigurieren, dass es ein digitales Zertifikat verwendet, das mit Embedded Security erstellt wurde. Wenn kein digitales Zertifikat verfügbar ist, müssen Sie eines von einer Zertifizierungsstelle beziehen. Anleitungen zur Konfiguration Ihres E-Mail-Programms und zum Bezug eines digitalen Zertifikats finden Sie in der Software-Hilfe Ihres E-Mail-Programms.

Allgemeine Aufgaben

Nachdem das allgemeine Benutzerkonto eingerichtet wurde, können Sie folgende Aufgaben ausführen:

- Verschlüsseln von Dateien und Ordnern
- Senden und Empfangen verschlüsselter E-Mails

Verwenden des persönlichen, sicheren Laufwerks

Nachdem Sie das PSD eingerichtet haben, werden Sie aufgefordert, das Kennwort für den allgemeinen Benutzerschlüssel bei der nächsten Anmeldung einzugeben. Wenn Sie das Kennwort für den allgemeinen Benutzerschlüssel richtig eingegeben haben, können Sie im Windows Explorer direkt auf das PSD zugreifen.

Verschlüsseln von Dateien und Ordnern

Beachten Sie bei der Arbeit mit verschlüsselten Dateien die folgenden Regeln:

- Sie können nur Dateien und Ordner in NTFS-Partitionen verschlüsseln. Dateien und Ordner in FAT-Partitionen können nicht verschlüsselt werden.
- Systemdateien und komprimierte Dateien können nicht verschlüsselt werden. Verschlüsselte Dateien können nicht komprimiert werden.
- Temporäre Ordner müssen verschlüsselt werden, weil sich Hacker für diese interessieren.
- Wenn Sie eine Datei oder einen Ordner erstmals verschlüsseln, wird automatisch eine Richtlinie für die Wiederherstellung eingerichtet. Diese Richtlinie gewährleistet, dass Sie bei Verlust der Verschlüsselungszertifikate und privaten Schlüssel einen Wiederherstellungs-Agent zum Entschlüsseln Ihrer Informationen verwenden können.

So verschlüsseln Sie Dateien und Ordner:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die bzw. den Sie verschlüsseln möchten.
2. Klicken Sie auf **Verschlüsseln**.
3. Klicken Sie auf eine der folgenden Optionen:
   - **Änderungen nur für diesen Ordner übernehmen.**
   - **Änderungen für diesen Ordner, untergeordnete Ordner und Dateien übernehmen.**
4. Klicken Sie auf **OK**.

Senden und Empfangen verschlüsselter E-Mails

Embedded Security ermöglicht das Senden und Empfangen verschlüsselter E-Mails. Der genaue Vorgang ist jedoch von dem Programm abhängig, mit dem Sie Ihre E-Mails bearbeiten. Weitere Informationen hierzu finden Sie in der Software-Hilfe von Embedded Security und Ihres E-Mail-Programms.

Ändern des Kennworts des einfachen Benutzerschlüssels

So ändern Sie das Kennwort des einfachen Benutzerschlüssels:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Security Manager**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Benutzereinstellungen**.
3. Klicken Sie im rechten Fensterbereich unter **Basic User password** (Kennwort des einfachen Benutzerschlüssels) auf **Ändern**.
4. Geben Sie zuerst das alte Kennwort ein. Geben Sie dann das neue Kennwort ein, und bestätigen Sie das neue Kennwort.
5. Klicken Sie auf **OK**.

Erweiterte Tasks

Administratoren können in Embedded Security die folgenden Aufgaben ausführen:

- Anmeldeinformationen, Embedded Security-Einstellungen und PSDs (Personal Secure Drives, Persönliche sichere Laufwerke) sichern und wiederherstellen
- Kennwort des Eigentümers ändern
- Benutzerkennwort zurücksetzen
- Sicherheitsanmeldeinformationen des Benutzers auf sichere Weise von einer Quellplattform auf eine Zielplattform migrieren

Sichern und Wiederherstellen

Mit der Sicherungsfunktion von Embedded Security erstellen Sie ein Archiv, das Zertifizierungsinformationen enthält, die bei einem Notfall wiederhergestellt werden.

Erstellen einer Sicherungsdatei

So erstellen Sie eine Sicherungsdatei:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fensterbereich auf **Konfigurieren**. HP Embedded Security for ProtectTools wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Wiederherstellen von Daten aus der Sicherungsdatei

So stellen Sie die Daten aus der Sicherungsdatei wieder her:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Sicherung**.
3. Klicken Sie im rechten Fensterbereich auf **Alle wiederherstellen**. HP Embedded Security for ProtectTools wird geöffnet.
4. Folgen Sie den Anleitungen auf dem Bildschirm.

Ändern des Eigentümerkennworts

Administratoren können das Kennwort des Eigentümers ändern:

1. Klicken Sie auf **Start**, **Alle Programme**, **HP** und anschließend auf **HP ProtectTools Administrator-Konsole**.
2. Klicken Sie im linken Fensterausschnitt auf **Embedded Security** und dann auf **Erweitert**.
3. Klicken Sie im rechten Fensterausschnitt unter **Owner Password** (Eigentümerkennwort) auf **Ändern**.
4. Geben Sie zuerst das alte Eigentümerkennwort ein. Geben Sie dann das neue Eigentümerkennwort ein, und bestätigen Sie das neue Kennwort.
5. Klicken Sie auf **OK**.

Erneutes Einrichten eines Benutzerkennworts

Der Administrator kann Benutzer beim Zurücksetzen vergessener Kennwörter unterstützen. Weitere Informationen finden Sie in der Software-Hilfe.

Migrieren von Schlüsseln mithilfe des Migrationsassistenten

Bei der Migration handelt es sich um eine erweiterte Administratoraufgabe. Sie ermöglicht das Verwalten, Wiederherstellen und Übertragen von Schlüsseln und Zertifikaten.

Weitere Informationen zur Migration finden Sie in der Software-Hilfe von Embedded Security.

11 Ausnahmen für lokalisierte Kennwörter

Auf der Ebene von Pre-Boot Security bzw. HP Drive Encryption wird die Kennwortlokalisierung nur beschränkt unterstützt. Dies wird in den folgenden Abschnitten beschrieben.

Windows IMEs werden weder auf der Ebene von Pre-Boot Security noch auf der Ebene von HP Drive Encryption unterstützt.

In Windows kann der Benutzer mit einem IME (Input Method Editor, Eingabemethoden-Editor) komplexe Zeichen und Symbole wie beispielsweise japanische oder chinesische Zeichen über eine westliche Standardtastatur eingeben.

IMEs werden weder auf der Ebene von Pre-Boot Security noch auf der Ebene von HP Drive Encryption unterstützt. Ein IME kann nicht dazu verwendet werden, ein Windows Kennwort im Anmeldebildschirm für Pre-Boot Security oder HP Drive Encryption einzugeben. Die Eingabe über einen IME kann zu einer Sperrung führen. In manchen Fällen zeigt Microsoft® Windows den IME nicht an, wenn der Benutzer das Kennwort eingibt.

Bei manchen japanischen Installationen von Windows XP heißt der Standard-IME für Japanisch beispielsweise Microsoft IME Standard 2002. Dies entspricht dem Tastaturlayout E0010411. Hier handelt es sich jedoch um einen IME und nicht ein Tastaturlayout. (Das Tastaturlayout-Kodierungsschema wird von Microsoft nur für IMEs verwendet, die das Konzept eines Tastaturlayouts erweitern). Da es sich hier nicht um ein Tastaturlayout handelt, das in der Eingabeumgebung der Kennwort-Eingabeaufforderung für BIOS Pre-Boot Security oder HP Drive Encryption dargestellt werden kann, werden alle mit diesem IME eingegebenen Kennwörter von HP ProtectTools abgelehnt. Microsoft IME Standard 2002 für Japanisch unterscheidet sich auch von dem „gemeinsamen Namen“ in Microsoft Windows Vista®. Windows weist einige IMEs einem Tastaturlayout zu. In solchen Fällen unterstützt HP ProtectTools den IME, da die zugrunde liegende Tastaturlayoutdefinition (der Hexadezimalcode) verwendet wird.

Die Lösung besteht darin, eines der folgenden unterstützten Tastaturlayouts auszuwählen, die dem Tastaturlayout 00000411 entsprechen:

- Microsoft IME für Japanisch
- Das japanische Tastaturlayout
- Office 2007 IME für Japanisch – Wenn Microsoft oder ein Dritter den Begriff IME oder Input Method Editor verwendet, handelt es sich bei der Eingabemethode nicht unbedingt um einen IME. Dies kann zu Verwirrung führen, aber die Software liest die Darstellung des Hexadezimalcodes. Aus diesem Grund kann HP ProtectTools die Konfiguration unterstützen, wenn ein IME einem unterstützten Tastaturlayout zugeordnet ist.

⚠ **VORSICHT!** Wenn HP ProtectTools bereitgestellt wurde, werden mit Windows IME eingegebene Kennwörter abgelehnt.

Ändern des Kennworts mit einem Tastaturlayout, das ebenfalls unterstützt wird

Wenn das Kennwort beispielsweise zunächst mit einem Tastaturlayout für US-Englisch (409) festgelegt wird und der Benutzer anschließend das Kennwort mit einem anderen Tastaturlayout ändert, das ebenfalls unterstützt wird, wie z. B. Lateinamerikanisches Spanisch (080A), funktioniert die Kennwortänderung zwar in HP Drive Encryption, jedoch nicht im BIOS, wenn der Benutzer Zeichen des spanischen Tastaturlayouts verwendet, die im amerikanischen Layout nicht vorhanden sind (zum Beispiel ē).

HINWEIS: Administratoren können dieses Problem lösen, indem sie die Funktion **Benutzer verwalten** in HP ProtectTools verwenden, das gewünschte Tastaturlayout im Betriebssystem auswählen und anschließend den Installations-Assistenten für Security Manager für den gleichen Benutzer erneut ausführen. Das gewünschte Tastaturlayout wird im BIOS gespeichert, und Kennwörter, die mit diesem Tastaturlayout eingegeben werden können, werden im BIOS korrekt festgelegt.

Ein weiteres potenzielles Problem ist die Verwendung verschiedener Tastaturlayouts, die die gleichen Zeichen erzeugen können. So kann sowohl mit dem Tastaturlayout US-International (20409) als auch mit dem lateinamerikanischen Tastaturlayout (080A) das Zeichen é erzeugt werden, obwohl dafür möglicherweise eine unterschiedliche Abfolge von Tasten gedrückt werden muss. Wird ein Kennwort zunächst mit dem lateinamerikanischen Tastaturlayout festgelegt, so ist das lateinamerikanische Tastaturlayout im BIOS eingestellt. Dies ist auch dann der Fall, wenn das Kennwort anschließend mit dem Tastaturlayout US-International geändert wird.

Behandeln von Sonderzeichen

- Chinesisch, Slowakisch, kanadisches Französisch und Tschechisch

  Wenn ein Benutzer eines der oben genannten Tastaturlayouts auswählt und dann ein Kennwort (beispielsweise abcdef) eingibt, muss in BIOS Pre-Boot Security oder HP Drive Encryption das gleiche Kennwort eingegeben werden, während die Umschalttaste für Kleinschreibung bzw. die Umschalttaste und die Feststelltaste für Großschreibung gedrückt werden. Bei der Eingabe von numerischen Kennwörtern muss der Nummernblock verwendet werden.

- Koreanisch

  Wenn ein Benutzer ein koreanisches Tastaturlayout auswählt und dann ein Kennwort eingibt, muss in BIOS Pre-Boot Security oder HP Drive Encryption das gleiche Kennwort eingegeben werden, während die rechte alt-Taste für Kleinschreibung und die rechte alt-Taste und die Feststelltaste für Großschreibung gedrückt werden.

- Die nicht unterstützten Zeichen sind in der folgenden Tabelle aufgeführt:

Sprache	Windows	BIOS	Drive Encryption
Arabisch	Die Tasten ﻹ ,ﻵ und ﻷ erzeugen zwei Zeichen.	Die Tasten ﻹ ,ﻵ und ﻷ erzeugen ein Zeichen.	Die Tasten ﻹ ,ﻵ und ﻷ erzeugen ein Zeichen.
Französisch (Kanada)	ç, è, à und é mit Feststelltaste entsprechen Ç, È, À und É in Windows.	ç, è, à und é mit Feststelltaste entsprechen ç, è, à und é in der BIOS Pre-Boot Security.	ç, è, à und é mit Feststelltaste entsprechen ç, è, à und é in HP Drive Encryption.
Spanisch	40a wird zwar nicht unterstützt, funktioniert aber trotzdem, da es von der Software zu c0a konvertiert wird. Aufgrund geringfügiger Unterschiede zwischen den Tastaturlayouts wird jedoch empfohlen, dass Spanisch sprechende Benutzer zum Tastaturlayout 1040a (spanische Variation) oder 080a (lateinamerikanisches Spanisch) wechseln.	N/V	N/V
US-International	◦ Die Tasten ¡, ¤, ‘, ’, ¥ und × in der oberen Reihe werden abgelehnt. ◦ Die Tasten å, ® und Þ in der zweiten Reihe werden abgelehnt. ◦ Die Tasten á, ð und ø in der dritten Reihe werden abgelehnt. ◦ Die Taste æ in der unteren Reihe wird abgelehnt.	N/V	N/V

Sprache	Windows	BIOS	Drive Encryption
Tschechisch	◦ Die Taste ģ wird abgelehnt. ◦ Die Taste į wird abgelehnt. ◦ Die Taste ų wird abgelehnt. ◦ Die Tasten ė, ı und ż werden abgelehnt. ◦ Die Tasten ģ, ķ, ļ, ņ und ŗ werden abgelehnt.	N/V	N/V
Slowakisch	Die Taste ż wird abgelehnt.	◦ Die Tasten š, ś und ş werden abgelehnt, wenn sie über die Tastatur eingegeben werden, jedoch bei Eingabe über die Bildschirmtastatur angenommen. ◦ Die unbelegte Taste ţ erzeugt zwei Zeichen.	N/V
Ungarisch	Die Taste ż wird abgelehnt.	Die Taste ţ erzeugt zwei Zeichen.	N/V

Sprache	Windows	BIOS	Drive Encryption
Slowenisch	Die Taste żŻ wird in Windows abgelehnt, und die alt-Taste erzeugt im BIOS eine unbelegte Taste.	Die Tasten ú, Ú, ů, Ů, ş, Ş, ś, Ś, š und Š werden im BIOS abgelehnt.	N/V
Japanisch	Nur unter Windows XP wird das Standard-Tastaturlayout für Japanisch (411) voll unterstützt. Für einen IME, normalerweise unter Windows XP als Microsoft Standard IME 2002 dargestellt, wird normalerweise keine Unterstützung geboten. Empirische Tests haben jedoch gezeigt, dass dieser IME und das Tastaturlayout 411 fast identisch sind, wenn einfache Zeichen eingegeben werden. Aus diesem Grund wechselt die Software bei diesem IME zum Tastaturlayout 411, wenn lokalisierte japanische Kennwörter zur Sicherung vom BIOS und HP Drive Encryption verwendet werden. Wenn verfügbar, sollte Microsoft Office 2007 IME verwendet werden. Trotz des IME-Namens handelt es sich hier um das unterstützte Tastaturlayout 411.	N/V	N/V

Vorgehensweise, wenn das Kennwort abgelehnt wird

Kennwörter können aus folgenden Gründen abgelehnt werden:

- Ein Benutzer verwendet einen nicht unterstützten IME. Dies kommt häufig bei Doppelbyte-Sprachen vor (Koreanisch, Japanisch, Chinesisch). So beheben Sie dieses Problem:
    1. Klicken Sie auf **Start**, auf **Systemsteuerung** und anschließend auf **Regions- und Sprachoptionen**.
    2. Klicken Sie auf die Registerkarte **Sprachen**.
    3. Klicken Sie auf die Schaltfläche **Details**.
    4. Klicken Sie auf der Registerkarte **Einstellungen** auf die Schaltfläche **Hinzufügen**, um eine unterstützte Tastatur hinzuzufügen (US-Tastaturen unter dem chinesischen Eingabegebietsschema hinzufügen).
    5. Legen Sie die unterstützte Tastatur als Standard-Eingabegebietsschema fest.
    6. Starten Sie HP ProtectTools neu, und geben Sie dann das Kennwort erneut ein.
- Ein Benutzer verwendet ein nicht unterstütztes Zeichen. So beheben Sie dieses Problem:
    1. Ändern Sie das Windows -Kennwort, sodass es nur unterstützte Zeichen enthält. Die nicht unterstützten Zeichen sind im Abschnitt „Behandeln von Sonderzeichen“ auf Seite 119 aufgeführt.
    2. Führen Sie den Installations-Assistenten für Security Manager erneut aus, und geben Sie dann das neue Windows Kennwort ein.

Glossar

Administrator
Siehe *Windows Administrator*.

Aktivierung
Die Aufgabe, die durchgeführt werden muss, bevor auf die anderen Funktionen von Drive Encryption zugegriffen werden kann. Verwenden Sie den Installations-Assistenten von HP ProtectTools, um Drive Encryption zu aktivieren. Drive Encryption kann nur von einem Administrator aktiviert werden. Der Aktivierungsvorgang besteht aus dem Aktivieren der Software, dem Verschlüsseln des Laufwerks, dem Erstellen eines Benutzerkontos sowie dem Erstellen des ursprünglichen Sicherungs-Chiffrierschlüssels auf einem Wechselmediengerät.

Anmeldedaten
Ein Element innerhalb von Security Manager, das aus einem Benutzernamen und einem Kennwort besteht (und eventuell anderen ausgewählten Informationen), die zur Anmeldung bei Websites oder anderen Programmen verwendet werden können.

Anmeldeinformationen
Die Mittel, mit denen ein Benutzer seine Berechtigung für eine bestimmte Aufgebe während der Authentifizierung beweist.

ATM
Automatic Technology Manager. Bietet Netzwerkadministratoren die Möglichkeit, Systeme remote auf BIOS-Ebene zu verwalten.

Authentifizierung
Die Prüfung, ob ein Benutzer zur Durchführung einer Task wie Zugriff auf einen Computer, Ändern von Programmeinstellungen oder Abrufen gesicherter Daten autorisiert ist.

Authentifizierung beim Systemstart
Eine Sicherheitsfunktion, die beim Einschalten des Computers eine Art von Authentifizierung erfordert, wie eine Smart Card, einen Sicherheitschip oder ein Kennwort.

Automatisches Shreddern
Geplante Shred-Vorgänge, die der Benutzer in File Sanitizer festlegt.

Benutzer
Jede bei Drive Encryption registrierte Person. Nicht-Administratoren verfügen nur über eingeschränkte Rechte in Drive Encryption. Benutzer können sich nur (mit Genehmigung des Administrators) registrieren und anmelden.

Biometrisch
Kategorie der Authentifizierungsinformationen, die eine physische Komponente, wie z. B. einen Fingerabdruck, beinhalten, um den Benutzer zu identifizieren.

Dashboard

Eine zentrale Schnittstelle, über die Sie auf die Merkmale und Einstellungen von HP ProtectTools Security Manager zugreifen und sie verwalten können.

Datenbestand
Eine Datenkomponente, die aus persönlichen Informationen oder Dateien, Verlaufsdaten und Internet-bezogenen Daten usw. besteht und sich auf der Festplatte befindet.

Digitale Signatur
Mit einer Datei gesendete Daten, die den Absender des Materials verifizieren und überprüfen, ob die Datei nach der Unterschrift geändert wurde.

Digitales Zertifikat
Elektronische Anmeldeinformationen, die die Identität einer Person oder eines Unternehmens durch Verknüpfung der Identität des Besitzers des digitalen Zertifikats mit zwei elektronischen Kennwörtern, die zum Unterschreiben digitaler Informationen verwendet werden, bestätigen.

Domäne
Eine Gruppe von Computern, die Teil eines Netzwerks sind und gemeinsam eine Verzeichnisdatenbank benutzen. Domänen sind einheitlich benannt, und jede verfügt über allgemeine Regeln und Prozeduren.

Drive Encryption
Schützt Ihre Daten, indem Ihre Festplatte(n) verschlüsselt wird/werden und somit die Informationen für Benutzer ohne entsprechende Berechtigung unlesbar werden.

Drive Encryption Anmeldebildschirm
Ein Logo-Bildschirm, der angezeigt wird, bevor Windows startet. Benutzer müssen ihren Windows Benutzernamen und das Kennwort oder ihre Smart Card-PIN eingeben oder mit dem registrierten Finger über den Sensor streichen. In den meisten Fällen ermöglicht die Eingabe der korrekten Informationen auf dem Drive Encryption-Anmeldebildschirm den direkten Zugriff auf Windows ohne die erneute Anmeldung auf dem Windows Anmeldebildschirm.

DriveLock
Eine Sicherheitsfunktion, die die Festplatte mit einem Benutzer verknüpft, der das DriveLock-Kennwort beim Computerstart dann korrekt eingeben muss.

Einfaches Löschen
Das Löschen des Windows Verweises zu einem Datenbestand. Der Inhalt des Datenbestands verbleibt auf der Festplatte, bis die Daten beim Überschreiben von freiem Speicherplatz überschrieben werden.

Einladung an vertrauenswürdige Kontakte
Eine E-Mail-Nachricht, die an eine Person gesendet wird, um sie zu bitten, ein vertrauenswürdiger Kontakt zu werden.

Empfänger einer Einladung an vertrauenswürdige Kontakte
Eine Person, die die Einladung erhält, einer vertrauenswürdiger Kontakt zu werden.

Empfohlener Signierer
Ein Benutzer, den der Eigentümer eines Microsoft Word oder Microsoft Excel Dokuments für das Hinzufügen einer Signaturzeile zu dem Dokument benennt.

Encryption File System (EFS)
Ein System, das alle Dateien und Unterordner innerhalb des ausgewählten Ordners verschlüsselt.

Entschlüsselung
Eine in der Kryptographie verwendete Prozedur zur Konvertierung von verschlüsselten Daten in Klartext.

Fingerabdruck

Eine digitale Extraktion Ihres Fingerabdruck-Abbilds. Das Fingerabdruck-Abbild selbst wird nie von Security Manager gespeichert.

Geräteklasse
Alle Geräte eines bestimmten Typs, beispielsweise Laufwerke.

Gerätezugriffsrichtlinie
Die Liste mit den Geräten, für die ein Benutzer ein Zugriffsrecht oder kein Zugriffsrecht besitzt.

Gruppe
Eine Benutzergruppe, der dasselbe Zugriffrecht für eine Geräteklasse oder ein bestimmtes Gerät gewährt oder verweigert wird.

Hintergrunddienst
Der Hintergrunddienst „HP ProtectTools Gerätesperre/Überwachung“ muss ausgeführt werden, damit die Richtlinien für die Gerätezugriffssteuerung zur Anwendung kommen. Sie können den Dienst in der Systemsteuerung über die Option „Verwaltung“ in der Anwendung „Dienste“ anzeigen. Wenn der Dienst nicht ausgeführt wird, versucht HP ProtectTools Security Manager, ihn zu starten, wenn die Richtlinien für die Gerätezugriffssteuerung angewendet werden.

HP SpareKey
Eine Wiederherstellungskopie des Drive Encryption-Schlüssels.

ID-Card
Windows Desktop-Minianwendung, mit der Ihr Desktop anhand Ihres Benutzernamens und eines ausgewählten Bildes visuell identifiziert werden kann. Klicken Sie auf die ID-Card, um HP ProtectTools Administrator-Konsole zu öffnen.

Identität
In HP ProtectTools Security Manager eine Gruppe von Anmeldedaten und Einstellungen, die wie ein Konto oder ein Profil für einen bestimmten Benutzer gehandhabt werden.

JITA
Just-In-Time-Authentifizierung.

Konsole
Eine zentrale Schnittstelle, über die Sie auf die Merkmale und Einstellungen von HP ProtectTools Administrator-Konsole zugreifen und sie verwalten können.

Kryptographie
Das Ver- und Entschlüsseln von Daten, damit diese nur von bestimmten Personen decodiert werden können.

Kryptographiediensteanbieter (Cryptographic Service Provider = CSP)
Ein Dienstanbieter oder eine Bibliothek von Verschlüsselungsalgorithmen, die in einer gut definierten Schnittstelle dazu benutzt werden können, bestimmte Verschlüsselungsfunktionen auszuüben.

Liste der vertrauenswürdigen Kontakte
Eine Liste der vertrauenswürdigen Kontakte.

Manuelles Shreddern
Das sofortige Shreddern eines Datenbestands oder ausgewählter Datenbestände unter Umgehung des Zeitplans für automatisches Shreddern.

Migration
Eine Aufgabe, die das Verwalten, Wiederherstellen und Übertragen von Privacy Manager Zertifikaten und vertrauenswürdigen Kontakten ermöglicht.

Netzwerkkonto

Ein Konto eines Benutzers oder Administrators unter Windows, entweder auf einem lokalen Computer, in einer Arbeitsgruppe oder einer Domäne.

Neustart
Der Neustart des Computers.

Notfallwiederherstellungsarchiv
Ein geschützter Speicherbereich, der die Neuverschlüsselung der einfachen Benutzerschlüssel von einem Plattform-Eigentümerschlüssel zu einem anderen ermöglicht.

PIN
Persönliche Identifikationsnummer.

PKI
Der Public Key Infrastructure-Standard, der die Schnittstellen für die Erstellung, Verwendung und Verwaltung von Zertifikaten und kryptographischen Schlüsseln definiert.

Privacy Manager Zertifikat
Ein digitales Zertifikat, das jedes Mal eine Authentifizierung erforderlich macht, wenn es zur Verschlüsselung verwendet wird, z. B. um E-Mail-Nachrichten und Microsoft Office Dokumente zu signieren und zu verschlüsseln.

PSD
PSD-Laufwerk (Personal Secure Drive). Bietet einen geschützten Speicherbereich für sensible Daten.

SATA-Gerätemodus
Ein Datenübertragungsmodus zwischen einem Computer und Massenspeichergeräten wie Festplatten und optischen Laufwerken.

Schaltfläche „Sicher Senden“
Eine Softwareschaltfläche in der Symbolleiste von Microsoft Outlook-E-Mail-Nachrichten. Klicken Sie auf diese Schaltfläche, um eine Microsoft Outlook-E-Mail-Nachricht zu signieren und/oder zu verschlüsseln.

Schaltfläche „Signieren und verschlüsseln“
Eine Schaltfläche, die auf der Symbolleiste der Microsoft Office-Anwendungen angezeigt wird. Durch Klicken auf die Schaltfläche können Sie ein Microsoft Office-Dokument signieren, verschlüsseln oder die Verschlüsselung von einem Microsoft Office-Dokument entfernen.

Shreddern
Die Ausführung eines Algorithmus, der die Daten in einem Datenbestand überschreibt.

Shred-Profil
Eine spezielle Löschmethode mit einer Liste von Datenbeständen.

Shred-Zyklus
Die Häufigkeit, mit der der Shred-Algorithmus für jeden Datenbestand ausgeführt wird. Je mehr Shred-Zyklen ausgeführt werden, desto sicherer ist der Computer.

Sicherheits-Anmeldemethode
Die Methode, mit der Benutzer sich auf dem Computer anmelden.

Sichern
Die Verwendung des Sicherungsmerkmals, um eine Kopie von wichtigen Programminformationen außerhalb des Programms zu speichern. Die Kopie kann zu einem späteren Zeitpunkt verwendet werden, um die Informationen auf demselben oder einem anderen Computer wiederherzustellen.

Signaturzeile

Ein Platzhalter zur optischen Markierung einer digitalen Signatur. Wenn ein Dokument signiert ist, werden der Name des Signierers und die Überprüfungsmethode angezeigt. Das Signierungsdatum und der Titel des Signierers können ebenfalls einbezogen werden.

Smart Card
Ein kleines Stück Hardware, in Größe und Form einer Kreditkarte ähnlich, auf dem identifizierende Informationen zum Eigentümer gespeichert sind. Dient zur Authentifizierung des Benutzers an einem Computer.

SSO (Single Sign On)
Eine Funktion, die Authentifizierungsinformationen speichert und es Ihnen ermöglicht, Security Manager für den Zugriff auf das Internet und auf Windows Anwendungen zu verwenden, die eine Kennwortauthentifizierung erfordern.

Szene
Ein Foto eines registrierten Benutzers, das zur Authentifizierung verwendet werden kann.

Tastenfolge
Eine Kombination aus bestimmten Tasten, die gedrückt wird, um einen automatischen Shred-Vorgang auszulösen, z. B. strg+alt+s.

Token
Siehe *Sicherheits-Anmeldemethode*.

TPM-Sicherheitschip (Trusted Platform Module)
Der allgemeine Ausdruck für den HP ProtectTools Embedded Security-Chip. Ein TPM-Chip authentifiziert einen Computer anstelle eines Benutzers, indem für das Host-System typische Informationen gespeichert werden, wie Verschlüsselungsschlüssel, digitale Zertifikate und Kennwörter. Ein TPM-Chip senkt das Risiko, dass die Informationen auf dem Computer durch Diebstahl oder einen Hackerangriff preisgegeben werden.

TXT
Trusted Execution Technology.

Überschreiben von freiem Speicherplatz
Das sichere Überschreiben gelöschter Datenbestände mit willkürlichen Daten, um den Inhalt der gelöschten Datenbestände unwiderruflich zu vernichten.

USB-Token
Ein Sicherheitsgerät, das identifizierende Informationen über einen Benutzer speichert. Wie eine Smart Card oder ein biometrisches Lesegerät wird es zur Authentifizierung des Benutzers bei einem Computer verwendet.

Verschlüsselung
Ein Verfahren ähnlich einer Algorithmusanwendung, das im Bereich der Kryptografie zur Umwandlung eines einfachen Texts in einen verschlüsselten Text angewendet wird, damit unbefugte Empfänger die darin enthaltenen Daten nicht lesen können. Es gibt viele verschiedene Arten der Datenverschlüsselung. Sie bilden die Basis für die Netzwerksicherheit. Zu den häufig verwendeten Verschlüsselungstechniken zählen die Standarddatenverschlüsselung und die Verschlüsselung mit einem öffentlichen Schlüssel.

Versiegeln für vertrauenswürdige Kontakte
Eine Aufgabe, die eine digitale Signatur hinzufügt, die E-Mail verschlüsselt und sie versendet, nachdem Sie sich mit der von Ihnen ausgewählten Sicherheits-Anmeldemethode authentifiziert haben.

Vertrauenswürdige Nachricht
Eine Kommunikationssitzung, während der vertrauenswürdige Nachrichten von einem vertrauenswürdigen Absender an eine vertrauenswürdigen Kontakt gesendet werden.

Vertrauenswürdiger Absender
Ein vertrauenswürdiger Kontakt, der signierte und/oder verschlüsselte E-Mails und Microsoft Office Dokumente versendet.

Vertrauenswürdiger Kontakt
Eine Person, die eine Einladung an vertrauenswürdige Kontakte angenommen hat.

Virtuelles Token
Eine Sicherheitsfunktion, die ähnlich einer Smart Card und einem Lesegerät funktioniert. Das Token wird entweder auf der Festplatte des Computers oder in der Registrierungsdatenbank von Windows gespeichert. Wenn Sie sich mit einem virtuellen Token anmelden, werden Sie nach einer Benutzer-PIN gefragt, um die Authentifizierung abzuschließen.

Widerruf-Kennwort
Ein Kennwort, das erstellt wird, wenn ein Benutzer ein digitales Zertifikat anfordert. Der Benutzer benötigt das Kennwort, um sein digitales Zertifikat zu widerrufen. Dadurch wird sichergestellt, dass nur der Benutzer in der Lage ist, das Zertifikat zu widerrufen.

Wiederherstellen
Ein Vorgang, bei dem Programminformationen von einer zuvor erstellten Sicherungsdatei in das entsprechende Programm kopiert werden.

Windows Administrator
Ein Benutzer mit umfassenden Rechten zum Ändern von Berechtigungen und Verwalten anderer Benutzer.

Windows Anmeldesicherheit
Schützt Ihr(e) Windows Konto/Konten, indem die Verwendung von bestimmten Anmeldedaten für den Zugriff erfordert wird.

Windows Benutzerkonto
Profil einer Person mit der Berechtigung, sich in einem Netzwerk oder an einem bestimmten Computer anzumelden.

Zertifizierungsstelle (CA)
Ein Service, der Zertifikate ausstellt, die zum Betreiben einer öffentlichen Schlüsselinfrastruktur erforderlich sind.

Index

T

U

V

W

Z



HP Notebook

Referenzhandbuch

Zweite Ausgabe: März 2011

Erste Ausgabe: Juni 2010

Teilenummer des Dokuments: 607195-042

Produkthinweis

In diesem Referenzhandbuch werden die Funktionen beschrieben, die von den meisten Modellen unterstützt werden. Einige der Funktionen stehen möglicherweise nicht auf Ihrem Computer zur Verfügung.

Sicherheitshinweis

VORSICHT! Um eventuelle Verbrennungen oder eine Überhitzung des Computers zu vermeiden, stellen Sie den Computer nicht direkt auf Ihren Schoß, und blockieren Sie die Lüftungsschlitze nicht. Verwenden Sie den Computer nur auf einer festen, ebenen Oberfläche. Vermeiden Sie die Blockierung der Luftzirkulation durch andere feste Objekte, wie beispielsweise einen in unmittelbarer Nähe aufgestellten Drucker, oder durch weiche Objekte, wie Kissen, Teppiche oder Kleidung. Das Netzteil sollte außerdem während des Betriebs nicht in Kontakt mit der Haut oder weichen Oberflächen, wie Kissen, Teppichen oder Kleidung, kommen. Der Computer und das Netzteil entsprechen den Temperaturgrenzwerten für dem Benutzer zugängliche Oberflächen, die durch den internationalen Standard für die Sicherheit von Einrichtungen der Informationstechnik (IEC 60950) definiert sind.

Inhaltsverzeichnis

1 Einführung

Dieses Handbuch enthält allgemeine Informationen zu HP Notebooks.

HINWEIS: Einige der in diesem Handbuch beschriebenen Funktionen stehen möglicherweise nicht auf Ihrem Computer zur Verfügung.

Weitere Informationen zu Ihrem neuen Computer

Die folgenden Benutzerhandbücher und Referenzmaterialien werden mit dem Computer geliefert, entweder in gedruckter Form, auf der Festplatte des Computers oder auf einer optischen Disc bzw. SD-Karte:

- Poster *Installationsanleitungen* – Hilft Ihnen bei der Einrichtung des Computers und beim Einschalten. Das Poster ist im Karton des Computers enthalten.

  HINWEIS: Informationen dazu, wo Sie Benutzerhandbücher und Referenzmaterial finden, erhalten Sie auf dem Poster.

- *Einführung* – Enthält Informationen zum Computer, einschließlich produktspezifischer Funktionen, Sicherung und Wiederherstellung, Wartung und technischer Daten.
- Hilfe und Support – Enthält Informationen zu Betriebssystem, Treiber, Tools zur Fehlerbeseitigung und technischen Support. Um auf Hilfe und Support zuzugreifen, wählen Sie **Start > Hilfe und Support**. Um landes- bzw. regionenspezifischen Support zu erhalten, gehen Sie zu http://www.hp.com/support, wählen Sie Ihr Land/Ihre Region, und folgen Sie den Anleitungen auf dem Bildschirm.
- *Handbuch für sicheres & angenehmes Arbeiten* – Hier werden die sachgerechte Einrichtung des Arbeitsplatzes sowie die richtige Haltung und gesundheitsbewusstes Arbeiten für Computerbenutzer beschrieben. Das Handbuch enthält auch wichtige Informationen zur elektrischen und mechanischen Sicherheit. Um auf dieses Handbuch zuzugreifen, wählen Sie **Start > Hilfe und Support > Benutzerhandbücher**. Das Handbuch ist auch im Web unter http://www.hp.com/ergo verfügbar.
- *Hinweise zu Zulassung, Sicherheit und Umweltverträglichkeit* – Enthält Sicherheits- und Zulassungsinformationen sowie Informationen zur Entsorgung von Akkus. Um auf die Hinweise zuzugreifen, wählen Sie **Start > Hilfe und Support > Benutzerhandbücher**.

2 Netzwerkfunktionen (bestimmte Modelle)

Ihr Computer unterstützt zwei Arten des Internetzugangs:

- **Wireless** – Informationen hierzu erhalten Sie unter „Herstellen einer Wireless-Verbindung“ auf Seite 2.
- **Kabelgebunden** – Informationen hierzu erhalten Sie unter „Herstellen einer Verbindung zu einem kabelgebundenen Netzwerk“ auf Seite 10.

HINWEIS: Bevor Sie eine Verbindung mit dem Internet herstellen können, müssen Sie einen Internetdienst einrichten.

Herstellen einer Wireless-Verbindung

Ihr Computer ist möglicherweise mit einem oder mehreren der folgenden Wireless-Geräte ausgestattet:

- Wireless Local Area Network (WLAN)-Gerät
- HP UMTS-Modul (WWAN-Gerät (Wireless Wide Area Network))
- Bluetooth® Gerät

Weitere Informationen zur Wireless-Technologie finden Sie in den Angaben und Website-Links unter Hilfe und Support.

Symbole für Wireless- und Netzwerkstatus

Windows® 7

Symbol	Name	Beschreibung
	Wireless (verbunden)	Zeigt an, dass ein oder mehrere Wireless-Geräte eingeschaltet sind.
	Wireless (getrennt)	Zeigt an, dass alle Wireless-Geräte ausgeschaltet sind.
	HP Connection Manager (bestimmte Modelle)	Öffnet HP Connection Manager. HP Connection Manager ermöglicht das Erstellen und Verwalten von WWAN-Verbindungen (bestimmte Modelle) sowie das Überprüfen des Status der WLAN- und Bluetooth-Verbindungen.

	Kabelgebundenes Netzwerk (verbunden)	Zeigt an, dass ein oder mehrere Netzwerkgeräte mit dem Netzwerk verbunden sind.
	Netzwerk (deaktiviert/getrennt)	Zeigt an, dass alle Netzwerkgeräte in der Windows Systemsteuerung deaktiviert sind.
	Netzwerk (verbunden)	Zeigt an, dass ein oder mehrere Netzwerkgeräte mit einem Netzwerk verbunden sind.
	Netzwerk (getrennt)	Zeigt an, dass Netzwerkgeräte nicht mit einem Netzwerk verbunden sind.
	Netzwerk (deaktiviert/getrennt)	Zeigt an, dass keine Wireless-Verbindungen verfügbar sind.

Windows Vista®

Symbol	Name	Beschreibung
	Wireless (verbunden)	Zeigt an, dass ein oder mehrere Wireless-Geräte eingeschaltet sind.
	Wireless (getrennt)	Zeigt an, dass alle Wireless-Geräte ausgeschaltet sind.
	HP Connection Manager (bestimmte Modelle)	Öffnet HP Connection Manager. HP Connection Manager ermöglicht das Erstellen und Verwalten von WWAN-Verbindungen (bestimmte Modelle) sowie das Überprüfen des Status der WLAN- und Bluetooth-Verbindungen.
	Wireless-Netzwerkverbindung (verbunden)	Zeigt an, dass ein oder mehrere WLAN-Geräte mit einem Netzwerk verbunden sind.
	Wireless-Netzwerkverbindung (getrennt)	Zeigt an, dass ein oder mehrere WLAN-Geräte nicht mit einem Netzwerk verbunden sind.
	Netzwerkstatus (verbunden)	Mit dem kabelgebundenen Netzwerk verbunden.
	Netzwerkstatus (getrennt)	Nicht mit dem kabelgebundenen Netzwerk verbunden.

Ein- oder Ausschalten von Wireless-Geräten

Sie können die Wireless-Taste oder HP Connection Manager (bestimmte Modelle) verwenden, um Wireless-Geräte ein- und auszuschalten.

HINWEIS: Der Computer verfügt möglicherweise über eine Wireless-Taste, einen Wireless-Schalter oder eine Wireless-Taste auf der Tastatur. Der Begriff Wireless-Taste wird in diesem Handbuch für alle Arten von Wireless-Bedienelementen verwendet. Informationen zur Position der Wireless-Taste am Computer finden Sie im Handbuch *Einführung*.

So schalten Sie Wireless-Geräte mithilfe von HP Connection Manager aus.

▲ Klicken Sie mit der rechten Maustaste auf das Symbol für HP Connection Manager im Infobereich außen rechts in der Taskleiste, und klicken Sie dann auf das Symbol „Ein-/ausschalten“ neben dem gewünschten Gerät.

– ODER –

Klicken Sie auf **Start > Alle Programme > HP > HP Connection Manager** und anschließend auf das Symbol „Ein-/ausschalten“ neben dem gewünschten Gerät.

Verwenden von HP Connection Manager (bestimmte Modelle)

HP Connection Manager ist ein zentrales Programm zum Verwalten Ihrer Wireless-Geräte, zum Herstellen einer Internetverbindung über HP Mobiles Internet sowie zum Senden und Empfangen von SMS (Text)-Nachrichten. Mit HP Connection Manager können Sie folgende Geräte verwalten:

- Wireless Local Area Network (WLAN)/WiFi
- Wireless Wide Area Network (WWAN)/HP Mobiles Internet
- Bluetooth®

HP Connection Manager bietet Informationen und Benachrichtigungen zu Verbindungsstatus, Stromversorgung, SIM-Karte und SMS-Nachrichten. Die Statusinformationen und Benachrichtigungen werden im Infobereich ganz rechts in der Taskleiste angezeigt.

So rufen Sie HP Connection Manager auf:

▲ Klicken Sie in der Taskleiste auf das Symbol HP Connection Manager.

– ODER –

Klicken Sie auf **Start > Alle Programme > HP > HP Connection Manager**.

Weitere Informationen finden Sie in der Hilfe zur HP Connection Manager Software.

Verwenden der Bedienelemente des Betriebssystems

Das Netzwerk- und Freigabecenter ermöglicht die Einrichtung einer Verbindung oder eines Netzwerks, die Verbindung mit einem Netzwerk, die Verwaltung von Wireless-Netzwerken sowie die Diagnose und Reparatur von Netzwerkproblemen.

So verwenden Sie die Bedienelemente des Betriebssystems:

▲ Wählen Sie **Start > Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter**.

Weitere Informationen finden Sie unter **Start > Hilfe und Support**.

Verwenden eines WLAN

Mit einer Wireless-Verbindung können Sie den Computer mit Wi-Fi-Netzwerken oder WLANs verbinden. Ein WLAN besteht aus anderen Computern und Zubehörgeräten, die per Wireless-Router oder Wireless-Access Point verbunden sind.

Anschließen des Computers an ein vorhandenes WLAN

Windows 7

1. Stellen Sie sicher, dass das WLAN-Gerät eingeschaltet ist. (Informationen hierzu erhalten Sie unter „Ein- oder Ausschalten von Wireless-Geräten“ auf Seite 4).
2. Klicken Sie im Infobereich außen rechts in der Taskleiste auf das Netzwerksymbol.
3. Wählen Sie aus der Liste Ihr WLAN aus.
4. Klicken Sie auf **Verbinden**.

   Wenn auf Ihrem WLAN eine Sicherheitsfunktion aktiviert ist, werden Sie aufgefordert, einen Netzwerksicherheitsschlüssel einzugeben. Geben Sie den Code ein, und klicken Sie dann auf **OK**, um die Verbindung herzustellen.

HINWEIS: Wenn keine WLANs aufgeführt sind, befinden Sie sich ggf. außerhalb der Reichweite eines Wireless-Routers oder Access Points.

HINWEIS: Wird das WLAN-Netzwerk, zu dem Sie eine Verbindung herstellen möchten, nicht angezeigt, klicken Sie auf **Netzwerk- und Freigabecenter öffnen**. Klicken Sie dann auf **Neue Verbindung oder neues Netzwerk einrichten**. Eine Liste von Optionen wird angezeigt. Sie können manuell nach einem Netzwerk suchen und die Verbindung herstellen oder eine neue Netzwerkverbindung einrichten.

Windows Vista

1. Stellen Sie sicher, dass das WLAN-Gerät eingeschaltet ist. (Informationen hierzu erhalten Sie unter „Ein- oder Ausschalten von Wireless-Geräten“ auf Seite 4.)
2. Wählen Sie **Start > Verbinden mit**.
3. Wählen Sie aus der Liste Ihr WLAN aus.
   - Wenn das Netzwerk ungesichert ist, wird eine Warnung angezeigt. Klicken Sie auf **Trotzdem verbinden**, um die Warnung zu akzeptieren und die Verbindung herzustellen.
   - Wenn auf Ihrem WLAN eine Sicherheitsfunktion aktiviert ist, werden Sie aufgefordert, einen Netzwerksicherheitsschlüssel einzugeben. Geben Sie den Code ein, und klicken Sie dann auf **Verbinden**, um die Verbindung herzustellen.

HINWEIS: Wenn keine WLANs aufgeführt sind, befinden Sie sich ggf. außerhalb der Reichweite eines Wireless-Routers oder Access Points.

HINWEIS: Wird das WLAN-Netzwerk, zu dem Sie eine Verbindung herstellen möchten, nicht angezeigt, klicken Sie auf **Alle Verbindungen anzeigen**. Es wird eine Liste mit den verfügbaren Netzwerken angezeigt. Sie können eine Verbindung zu einem bestehenden Netzwerk herstellen oder eine neue Netzwerkverbindung einrichten.

Nachdem die Verbindung hergestellt wurde, platzieren Sie den Mauszeiger auf dem Netzwerksymbol im Infobereich außen rechts in der Taskleiste, um den Namen und den Status der Verbindung zu überprüfen.

HINWEIS: Die Reichweite von Wireless-Signalen hängt von der WLAN-Implementierung, dem Router-Hersteller sowie Störungen durch andere elektronische Geräte oder bauliche Hindernisse wie Wände und Böden ab.

Einrichten eines neuen WLAN

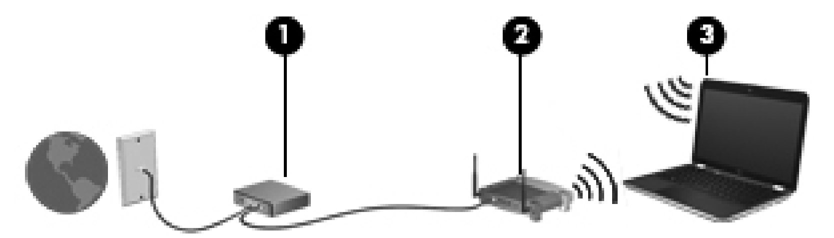
Benötigte Geräte:

- Ein separat erhältliches Breitbandmodem (DSL oder Kabel) **(1)** sowie eine Hochgeschwindigkeits-Internetanbindung über einen Internet-Serviceanbieter (ISP)
- Einen Wireless-Router (separat zu erwerben) **(2)**

  HINWEIS: Einige Kabelmodems verfügen über einen integrierten Router. Wenden Sie sich an Ihren Internet-Serviceanbieter (ISP), um abzuklären, ob Sie einen separaten Router benötigen.

- Den wireless-fähigen Computer **(3)**

Die Abbildung zeigt ein Beispiel einer Wireless-Netzwerk-Installation mit Internetanschluss.



HINWEIS: Für das Einrichten einer Wireless-Verbindung müssen Computer und Wireless-Router synchronisiert sein. Um Computer und Wireless-Router zu synchronisieren, schalten Sie den Computer und den Wireless-Router aus und wieder ein.

Mit zunehmendem Netzwerkumfang können weitere wireless-fähige und kabelgebundene Computer für den Internetzugang an das Netzwerk angeschlossen werden.

Wenn Sie Hilfe beim Einrichten Ihres WLAN benötigen, ziehen Sie die Dokumentation von Ihrem Router-Hersteller oder Internet-Serviceanbieter zu Rate.

Schützen Ihres WLAN

Wenn Sie ein WLAN einrichten oder auf ein vorhandenes WLAN zugreifen, sollten Sie immer Sicherheitsfunktionen aktivieren, um Ihr Netzwerk vor unberechtigtem Zugriff zu schützen. WLANs in öffentlichen Bereichen (Hotspots) wie Cafés und Flughäfen bieten möglicherweise keine Sicherheit. Wenn Sie hinsichtlich der Sicherheit Ihres Computers Bedenken haben, beschränken Sie Ihre Netzwerkaktivitäten auf nicht vertrauliche E-Mail-Korrespondenz und Surfen im Internet auf bekannten Websites.

Wireless-Funksignale werden außerhalb des Netzwerks gesendet, deshalb können andere WLAN-Geräte ungeschützte Signale empfangen. Sie können folgende Vorsichtsmaßnahmen treffen, um Ihr WLAN zu schützen:

- **Firewall** – Eine Firewall überprüft an das Netzwerk gesendete Daten bzw. Datenanforderungen und blockiert verdächtige Elemente. Firewalls sind als Software und Hardware erhältlich. In einigen Netzwerken werden beide Arten verwendet.
- **Wireless-Verschlüsselung** – Wi-Fi Protected Access (WPA) verwendet Sicherheitseinstellungen, um die im Netzwerk gesendeten Daten zu verschlüsseln und entschlüsseln. WPA verwendet das Temporal Key Integrity Protocol (TKIP), um dynamisch für jedes Paket einen neuen Schlüssel zu generieren. Es werden darüber hinaus unterschiedliche Schlüsselsätze für jeden Computer im Netzwerk generiert.

Nutzung eines anderen Netzwerks (Roaming)

Wenn sich der Computer innerhalb der Reichweite eines anderen WLAN befindet, versucht Windows, eine Verbindung zu diesem Netzwerk herzustellen. Nach einem erfolgreichen Versuch ist der Computer automatisch mit dem neuen Netzwerk verbunden. Wenn Windows das neue Netzwerk nicht erkennt, gehen Sie nach demselben Verfahren vor, das Sie verwendet haben, um erstmalig eine Verbindung zu Ihrem WLAN herzustellen.

Verwenden von HP UMTS (bestimmte Modelle)

Mithilfe von HP UMTS kann Ihr Computer Wireless Wide Area Networks (WWANs) verwenden, um von mehr Orten oder aus größeren Entfernungen auf das Internet zuzugreifen, als dies bei der Verwendung von WLANs der Fall wäre. Um HP UMTS verwenden zu können, ist ein Netzwerk-Serviceanbieter erforderlich, wobei es sich in den meisten Fällen um einen Mobilfunk-Netzbetreiber handelt.

Wenn Sie einen Service eines Mobilfunk-Netzbetreibers nutzen, können Sie mit HP UMTS auf das Internet zugreifen, E-Mails senden oder eine Verbindung zu Ihrem Firmennetz herstellen, ohne dass Sie auf Wi-Fi-Hotspots angewiesen sind.

HINWEIS: Zur Aktivierung des UMTS-Dienstes benötigen Sie möglicherweise die HP UMTS-Modul-Seriennummer. Informationen dazu, wo Sie die Seriennummer finden, erhalten Sie im Handbuch *Einführung*.

Einige Mobilfunk-Netzbetreiber erfordern die Verwendung einer SIM-Karte (Subscriber Identity Module). Eine SIM-Karte enthält grundlegende Informationen wie eine persönliche Identifikationsnummer (PIN) sowie Netzwerkinformationen. Bei einigen Computern ist eine vorinstallierte SIM-Karte enthalten. Wenn keine SIM-Karte vorinstalliert ist, wird möglicherweise eine SIM-Karte zusammen mit den Informationen über HP UMTS im Lieferumfang Ihres Computers bereitgestellt, oder Sie erhalten eine SIM-Karte separat von Ihrem Mobilfunk-Serviceanbieter.

Informationen zum Einsetzen und Entfernen der SIM-Karte finden Sie unter „Einsetzen einer SIM-Karte“ auf Seite 8 und „Entfernen einer SIM-Karte“ auf Seite 9.

Informationen zu HP UMTS und zur Aktivierung des UMTS-Dienstes mit einem gewünschten Mobilfunk-Netzbetreiber finden Sie in den HP UMTS-Informationen, die im Lieferumfang Ihres Computers enthalten sind. Weitere Informationen finden Sie auf der HP Website unter http://www.hp.com/go/mobilebroadband (nur für USA).

Einsetzen einer SIM-Karte

HINWEIS: Informationen dazu, wo sich der SIM-Steckplatz befindet, erhalten Sie im Handbuch *Einführung*.

1. Schalten Sie den Computer aus. Wenn Sie sich nicht sicher sind, ob der Computer ausgeschaltet ist oder sich im Ruhezustand befindet, schalten Sie ihn durch Drücken der Betriebstaste ein. Fahren Sie ihn dann über das Betriebssystem herunter.
2. Schließen Sie das Display.
3. Trennen Sie alle externen Geräte, die an den Computer angeschlossen sind.
4. Ziehen Sie das Netzkabel aus der Steckdose.
5. Entfernen Sie den Akku.

6. Schieben Sie die SIM-Karte in den Steckplatz, und drücken Sie die SIM-Karte vorsichtig in den Steckplatz, bis sie fest sitzt.

   ACHTUNG: Setzen Sie die SIM-Karte so ein, wie es auf dem Symbol neben dem Steckplatz für die SIM-Karte dargestellt ist. Wenn die SIM-Karte falsch eingesetzt wird, kann die SIM-Karte oder der SIM-Anschluss beschädigt werden.

   Üben Sie beim Einsetzen einer SIM-Karte nur minimalen Druck aus, um das Risiko einer Beschädigung des Anschlusses zu minimieren.

7. Setzen Sie den Akku wieder ein.

   HINWEIS: HP UMTS wird deaktiviert, wenn der Akku nicht wieder eingesetzt wird.

8. Schließen Sie die externe Stromversorgung und Peripheriegeräte wieder an.
9. Schalten Sie den Computer ein.

Entfernen einer SIM-Karte

HINWEIS: Informationen dazu, wo sich der SIM-Steckplatz befindet, erhalten Sie im Handbuch *Einführung*.

1. Schalten Sie den Computer aus. Wenn Sie sich nicht sicher sind, ob der Computer ausgeschaltet ist oder sich im Ruhezustand befindet, schalten Sie ihn durch Drücken der Betriebstaste ein. Fahren Sie ihn dann über das Betriebssystem herunter.
2. Schließen Sie das Display.
3. Trennen Sie alle externen Geräte, die an den Computer angeschlossen sind.
4. Ziehen Sie das Netzkabel aus der Steckdose.
5. Entfernen Sie den Akku.
6. Drücken Sie die SIM-Karte vorsichtig nach innen, und nehmen Sie sie dann aus dem Steckplatz.
7. Setzen Sie den Akku wieder ein.
8. Schließen Sie die externe Stromversorgung und Peripheriegeräte wieder an.
9. Schalten Sie den Computer ein.

Verwenden von GPS (bestimmte Modelle)

Ihr Computer ist möglicherweise mit GPS (Global Positioning System) ausgestattet. Mit GPS ausgestattete Systeme können mithilfe von GPS-Satelliten Standort, Geschwindigkeit und Richtung bestimmen.

Weitere Informationen finden Sie in der Hilfe zu HP GPS and Location.

Verwenden von Bluetooth Geräten

Ein Bluetooth Gerät bietet Wireless-Kommunikation auf kurze Distanz, bei der die Kabelverbindung ersetzt wird, die herkömmlicherweise elektronische Geräte wie beispielsweise folgende Geräte verbindet:

- Computer
- Telefone
- Bildverarbeitungsgeräte (Kameras und Drucker)
- Audiogeräte

Bluetooth Geräte bieten Peer-to-Peer-Funktionen, die den Aufbau eines PAN (Personal Area Network) mit Bluetooth-fähigen Geräten ermöglichen. Weitere Informationen zur Konfiguration und Verwendung von Bluetooth Geräten finden Sie in der Hilfe zur Bluetooth Software.

Bluetooth und gemeinsame Nutzung der Internetverbindung (ICS)

HP rät davon ab, einen Computer mit Bluetooth als Host einzurichten und ihn als Gateway zu verwenden, über das andere Computer eine Verbindung zum Internet herstellen können. Wenn zwei oder mehr Computer über Bluetooth verbunden sind und auf einem der Computer die gemeinsame Nutzung der Internetverbindung aktiviert ist, können die anderen Computer über das Bluetooth Netzwerk keine Verbindung zum Internet herstellen.

Die Stärke von Bluetooth liegt darin, Datentransfers zwischen einem Computer und Wireless-Geräten, wie beispielsweise Mobiltelefonen, Druckern, Kameras und Handhelds, zu synchronisieren. Es ist jedoch nicht möglich, zwei oder mehr Computer dauerhaft miteinander zu verbinden, um das Internet über Bluetooth gemeinsam zu nutzen. Dies ist eine Einschränkung von Bluetooth und des Windows Betriebssystems.

Herstellen einer Verbindung zu einem kabelgebundenen Netzwerk

Verwenden eines Modems (bestimmte Modelle)

Ein Modem muss mit der analogen Telefonleitung über ein 6-adriges RJ-11-Modemkabel (separat erhältlich) verbunden werden. In einigen Ländern oder Regionen ist auch ein spezieller Modemkabeladapter erforderlich. Buchsen für digitale Nebenstellensysteme können analogen Telefonbuchsen ähneln, sind jedoch nicht mit dem Modem kompatibel.

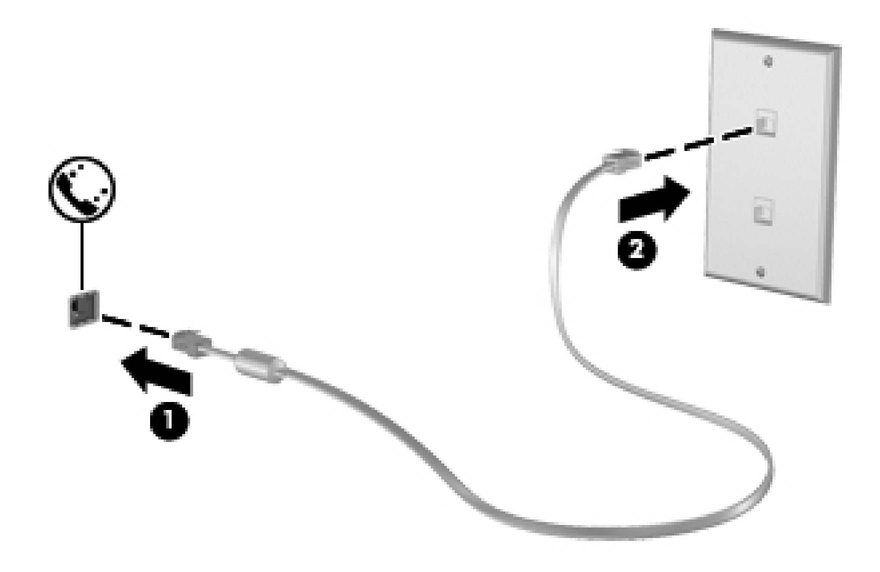
⚠ **VORSICHT!** Um Stromschlag- und Brandgefahr sowie eine Beschädigung der Geräte zu vermeiden, stecken Sie kein Modem- oder Telefonanschlusskabel in die RJ-45-Netzwerkbuchse.

Wenn das Modemkabel über eine Schaltung zur Rauschunterdrückung **(1)** verfügt, die Störungen durch Rundfunk- und Fernsehempfang verhindert, schließen Sie das Kabelende mit der Schaltung **(2)** am Computer an.



Anschließen eines Modemkabels

1. Stecken Sie das Modemkabel in die Modembuchse **(1)** am Computer.
2. Stecken Sie das Modemkabel in die RJ-11-Telefonbuchse **(2)** an der Wand.

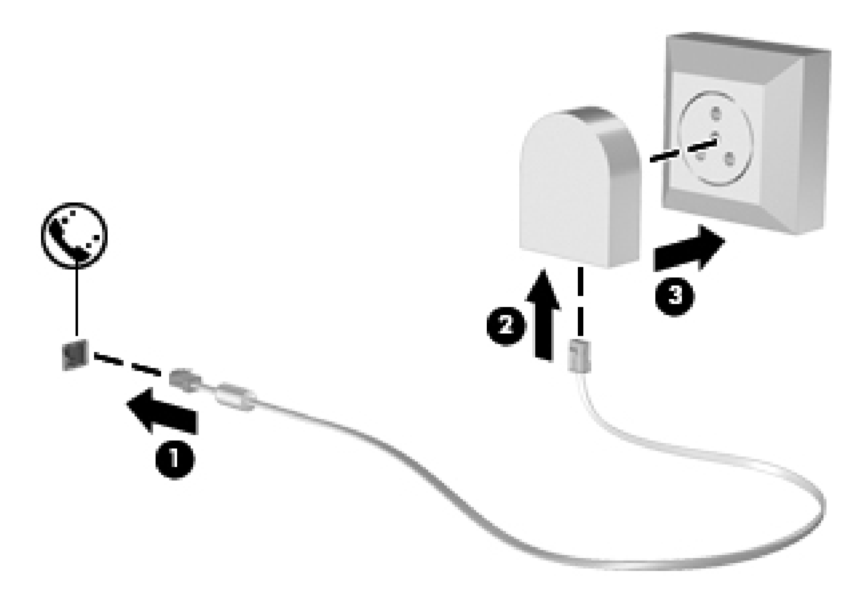


Anschließen eines landes- oder regionenspezifischen Modemkabeladapters

Telefonbuchsen sind je nach Land oder Region unterschiedlich. Um das Modem und Modemkabel außerhalb des Landes oder der Region, in der Sie den Computer erworben haben, zu verwenden, müssen Sie einen länder- oder regionenspezifischen Modemkabeladapter erwerben.

So schließen Sie das Modem an eine analoge Telefonleitung ohne RJ-11-Telefonbuchse an:

1. Stecken Sie das Modemkabel in die Modembuchse **(1)** am Computer.
2. Stecken Sie das Modemkabel in den Modemkabeladapter **(2)**.
3. Stecken Sie den Modemkabeladapter **(3)** in die Telefonbuchse an der Wand.



Auswählen der Standorteinstellung

Anzeigen der aktuellen Standortauswahl

Windows 7

1. Wählen Sie **Start > Systemsteuerung**.
2. Klicken Sie auf **Zeit, Sprache und Region**.
3. Klicken Sie auf **Region und Sprache**.
4. Klicken Sie auf die Registerkarte **Standort**, um Ihren Standort anzuzeigen.

Windows Vista

1. Wählen Sie **Start > Systemsteuerung**.
2. Klicken Sie auf **Zeit, Sprache und Region**.
3. Klicken Sie auf **Regions- und Sprachoptionen**.

   Ihr Ort wird unter Standort angezeigt.

Hinzufügen von neuen Standorten im Ausland

Auf neuen Computern ist die einzige für das Modem verfügbare Standorteinstellung die Einstellung für das Land oder die Region, in der Sie den Computer erworben haben. Wenn Sie in andere Länder oder Regionen verreisen, geben Sie für das interne Modem eine Standorteinstellung an, die den Betriebsstandards des Landes oder der Region entspricht, in dem/der Sie das Modem verwenden.

Wenn Sie neue Standorteinstellungen hinzufügen, werden Sie im Computer gespeichert, so dass Sie jederzeit zwischen verschiedenen Einstellungen wechseln können. Sie können mehrere Standorteinstellungen für ein Land oder eine Region hinzufügen.

ACHTUNG: Um das Risiko zu verringern, dass die Heimateinstellungen verloren gehen, löschen Sie die aktuellen Länder- oder Regionseinstellungen des Modems nicht. Um die Modemverwendung in anderen Ländern oder Regionen zu ermöglichen, ohne dass die Heimatkonfiguration verloren geht, fügen Sie für jeden Ort, in dem Sie das Modem verwenden wollen, eine neue Konfiguration hinzu.

ACHTUNG: Um das Risiko zu verringern, dass Sie das Modem auf eine Art konfigurieren, die die Telekommunikationsregelungen und Gesetze in dem besuchten Land oder der Region verletzen, wählen Sie das Land oder die Region, in dem/der sich der Computer befindet. Das Modem funktioniert unter Umständen nicht korrekt, wenn nicht die richtige Länder- oder Regionenauswahl getroffen wurde.

Windows 7

1. Wählen Sie **Start > Geräte und Drucker**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das für Ihren Computer steht, und wählen Sie anschließend **Modemeinstellungen**.

   HINWEIS: Sie müssen zuerst eine aktuelle Ortskennzahl festlegen, bevor die Registerkarte „Wählregeln“ angezeigt wird. Wenn Sie noch keinen Standort eingerichtet haben, werden Sie zur Eingabe des Standorts aufgefordert, wenn Sie auf die Modemeinstellungen klicken.

3. Klicken Sie auf die Registerkarte **Wählregeln**.
4. Klicken Sie auf **Neu**. Das Fenster für die Eingabe eines neuen Standorts wird geöffnet.
5. Geben Sie im Feld „Standortname“ einen Namen (z. B. `Zuhause` oder `Arbeit`) für die neue Standorteinstellung ein.
6. Wählen Sie ein Land bzw. eine Region aus der Liste „Land/Region“ aus. (Wenn Sie ein Land bzw. eine Region wählen, das bzw. die nicht durch das Modem unterstützt wird, wird Vereinigte Staaten von Amerika oder Großbritannien als Landes-/Regionenauswahl angezeigt.)
7. Geben Sie die Ortskennzahl, eine Amtskennziffer (falls erforderlich) und die Netzkennzahl (falls erforderlich) ein.
8. Klicken Sie neben „Wählverfahren“ auf **Ton (MFV)** oder **Impuls (IWV)**.
9. Klicken Sie auf **OK**, um die neue Standorteinstellung zu speichern.
10. Wählen Sie eine der folgenden Optionen:
    - Klicken Sie auf **OK**, um die neue Standorteinstellung als aktuellen Standort zu übernehmen.
    - Um eine andere Standorteinstellung als aktuelle Standorteinstellung auszuwählen, markieren Sie die gewünschte Einstellung in der Liste **Standort**, und klicken Sie anschließend auf **OK**.

HINWEIS: Sie können die vorherige Anleitung verwenden, um Standorteinstellungen für Orte innerhalb Ihres eigenen Landes oder Ihrer Region sowie in anderen Ländern oder Regionen hinzuzufügen. Beispielsweise können Sie eine `Arbeit` genannte Einstellung hinzufügen, die die Wählregeln für den Zugriff auf eine Amtsleitung beinhaltet.

Windows Vista

1. Wählen Sie **Start > Systemsteuerung**.
2. Klicken Sie auf **Hardware und Sound**.
3. Klicken Sie auf **Telefon- und Modemoptionen**.
4. Klicken Sie auf die Registerkarte **Wählregeln**.
5. Klicken Sie auf **Neu**. Das Fenster für die Eingabe eines neuen Standorts wird geöffnet.
6. Geben Sie im Feld „Standortname“ einen Namen (z. B. `Zuhause` oder `Arbeit`) für die neue Standorteinstellung ein.
7. Wählen Sie ein Land bzw. eine Region aus der Liste „Land/Region“ aus. (Wenn Sie ein Land bzw. eine Region wählen, das bzw. die nicht durch das Modem unterstützt wird, wird Vereinigte Staaten von Amerika oder Großbritannien als Landes-/Regionenauswahl angezeigt.)
8. Geben Sie die Ortskennzahl, eine Amtskennziffer (falls erforderlich) und die Netzkennzahl (falls erforderlich) ein.
9. Klicken Sie neben „Wählverfahren“ auf **Ton (MFV)** oder **Impuls (IWV)**.
10. Klicken Sie auf **OK**, um die neue Standorteinstellung zu speichern.
11. Wählen Sie eine der folgenden Optionen:
    - Klicken Sie auf **OK**, um die neue Standorteinstellung als aktuellen Standort zu übernehmen.
    - Um eine andere Standorteinstellung als aktuelle Standorteinstellung auszuwählen, markieren Sie die gewünschte Einstellung in der Liste „Standort“, und klicken Sie anschließend auf **OK**.

HINWEIS: Sie können die vorherige Anleitung verwenden, um Standorteinstellungen für Orte innerhalb Ihres eigenen Landes oder Ihrer Region sowie in anderen Ländern oder Regionen hinzuzufügen. Beispielsweise können Sie eine `Arbeit` genannte Einstellung hinzufügen, die die Wählregeln für den Zugriff auf einen Amtsanschluss beinhaltet.

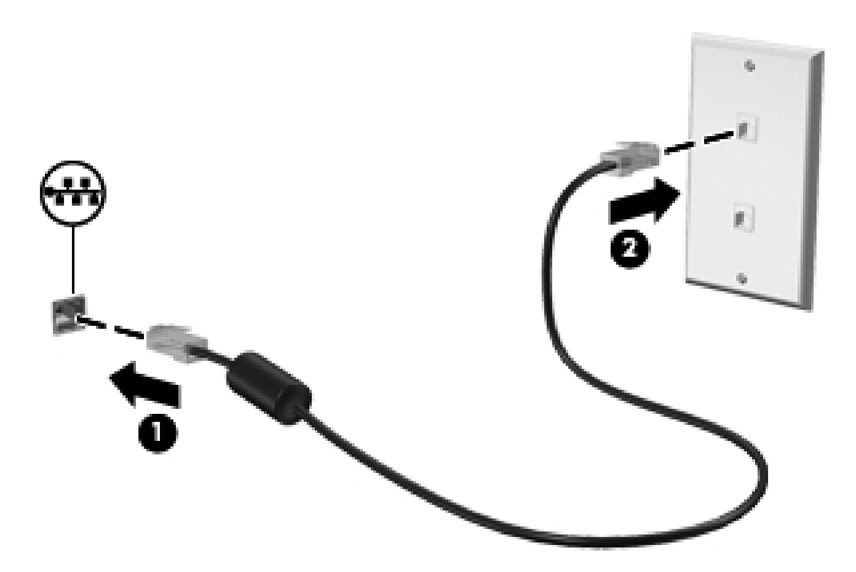
Herstellen einer Verbindung mit einem lokalen Netzwerk (LAN) (bestimmte Modelle)

Für die Verbindung mit einem LAN ist ein (separat erworbenes) 8-adriges RJ-45-Netzwerkkabel erforderlich. Wenn das Netzwerkkabel über eine Schaltung zur Rauschunterdrückung **(1)** verfügt, die Störungen durch Rundfunk- und Fernsehempfang verhindert, schließen Sie das Kabelende mit der Schaltung **(2)** am Computer an.



So schließen Sie das Netzwerkkabel an:

1. Stecken Sie das Netzwerkkabel in die Netzbuchse **(1)** am Computer.
2. Schließen Sie das Netzwerkkabel an eine Netzwerkdose an der Wand **(2)** an.



VORSICHT! Um das Risiko von Stromschlägen, Feuer oder Geräteschäden zu senken, stecken Sie kein Modem- oder Telefonkabel in eine RJ-45-Netzwerkbuchse.

3 Multimedia

Ihr Computer verfügt möglicherweise über folgende Komponenten:

- Integrierte(r) Lautsprecher
- Integrierte(s) Mikrofon(e)
- Integrierte Webcam
- Vorinstallierte Multimedia-Software
- Multimedia-Tasten

Verwenden der Tasten für die Medienwiedergabe

Je nach Computermodell stehen Ihnen die folgenden Tasten für die Medienwiedergabe zur Verfügung, mit denen Sie Mediendateien abspielen, unterbrechen, vor- oder zurückspulen können:

- Medientasten
- Medien-Tastenkombinationen (spezielle Tasten, die zusammen mit der fn-Taste gedrückt werden).
- Medientasten auf der Tastatur

Informationen zu den Tasten für die Medienwiedergabe am Computer finden Sie im Handbuch *Einführung*.

Audio

Auf Ihrem Computer können Sie verschiedene Audiofunktionen nutzen:

- Wiedergeben von Musik
- Audioaufnahmen
- Herunterladen von Musikdateien aus dem Internet
- Erstellen von Multimedia-Präsentationen
- Ton- und Bildübertragungen mit Instant Messaging Programmen
- Streaming von Radioprogrammen
- Erstellen (Brennen) von Audio-CDs mit dem installierten optischen Laufwerk (bestimmte Modelle) oder auf einem optionalen externen optischen Laufwerk (separat erhältlich)

Einstellen der Lautstärke

Je nach Computermodell stehen Ihnen zum Einstellen der Lautstärke folgende Möglichkeiten zur Verfügung:

- Lautstärketasten
- Medien-Tastenkombinationen (spezielle Tasten, die zusammen mit der fn-Taste gedrückt werden).
- Lautstärketasten auf der Tastatur

VORSICHT! Reduzieren Sie zur Vermeidung von Gesundheitsschäden die Lautstärke, bevor Sie Kopfhörer, Ohrhörer oder ein Headset verwenden. Zusätzliche Sicherheitsinformationen finden Sie im Dokument *Hinweise zu Zulassung, Sicherheit und Umweltverträglichkeit*.

HINWEIS: Die Lautstärke kann auch über das Betriebssystem und eine Reihe anderer Programme eingestellt werden.

HINWEIS: Informationen zu den am Computer verfügbaren Lautstärkeregelungsmöglichkeiten finden Sie im Handbuch *Einführung*.

Überprüfen der Audiofunktionen auf dem Computer

HINWEIS: Die besten Ergebnisse bei einer Aufnahme erzielen Sie in einer leisen Umgebung und wenn Sie direkt in das Mikrofon sprechen.

Windows 7

So überprüfen Sie die Audiofunktionen auf Ihrem Computer:

1. Wählen Sie **Start > Systemsteuerung > Hardware und Sound > Sound**.
2. Das Fenster „Sound“ wird geöffnet. Klicken Sie auf die Registerkarte **Sounds**. Wählen Sie unter „Programmereignisse“ ein beliebiges Tonereignis wie einen Piep- oder einen Signalton aus, und klicken Sie auf die Schaltfläche **Test**.

   Der Ton sollte über die Lautsprecher oder angeschlossenen Kopfhörer zu hören sein.

So überprüfen Sie die Aufnahmefunktionen auf Ihrem Computer:

1. Wählen Sie **Start > Alle Programme > Zubehör > Audiorecorder**.
2. Klicken Sie auf **Aufnahme beginnen**, und sprechen Sie in das Mikrofon. Speichern Sie die Datei auf dem Desktop.
3. Öffnen Sie ein Multimedia-Programm, und geben Sie die Aufnahme wieder.

Um die Audioeinstellungen auf dem Computer zu bestätigen oder zu ändern, wählen Sie **Start > Systemsteuerung > Hardware und Sound > Sound**.

Windows Vista

So überprüfen Sie die Audiofunktionen auf Ihrem Computer:

1. Wählen Sie **Start > Systemsteuerung > Hardware und Sound > Sound**.
2. Das Fenster „Sound“ wird geöffnet. Klicken Sie auf die Registerkarte **Sounds**. Wählen Sie unter „Programm“ ein beliebiges Klangereignis wie einen Piep- oder einen Signalton, und klicken Sie auf die Schaltfläche **Test**.

   Der Ton sollte über die Lautsprecher oder angeschlossenen Kopfhörer zu hören sein.

So überprüfen Sie die Aufnahmefunktionen auf Ihrem Computer:

1. Wählen Sie **Start > Alle Programme > Zubehör > Audiorecorder**.
2. Klicken Sie auf **Aufnahme beginnen**, und sprechen Sie in das Mikrofon. Speichern Sie die Datei auf dem Desktop.
3. Öffnen Sie ein Multimedia-Programm, und geben Sie die Aufnahme wieder.

Um die Audioeinstellungen auf dem Computer zu bestätigen oder zu ändern, wählen Sie **Start > Systemsteuerung > Audio**.

Webcam (bestimmte Modelle)

Bei einigen Computern ist eine Webcam integriert. Mithilfe der vorinstallierten Software können Sie mit der Webcam Fotos aufnehmen und Videos aufzeichnen. Anschließend können Sie eine Vorschau der Fotos und Videos anzeigen und die Aufnahmen speichern.

Die Webcam-Software bietet die folgenden Funktionen:

- Aufzeichnen und gemeinsames Nutzen von Videos
- Video-Streaming mit Instant Messaging-Software
- Aufnehmen von Fotos

Informationen zum Zugriff auf die Webcam erhalten Sie im Handbuch *Einführung*. Informationen zur Verwendung der Webcam finden Sie unter **Start > Hilfe und Support**.

Video

Ihr Computer ist möglicherweise mit einem oder mehreren der folgenden Anschlüsse für externe Videogeräte ausgestattet:

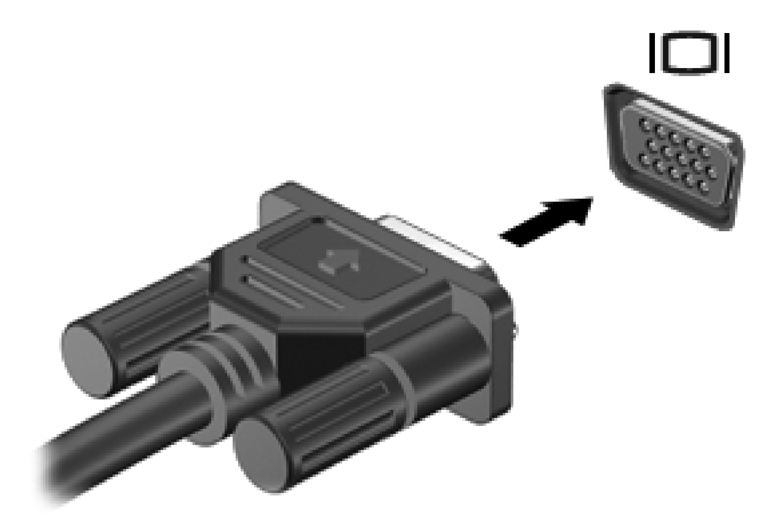
- VGA
- HDMI (High Definition Multimedia Interface)

HINWEIS: Informationen zu den Videoanschlüssen am Computer finden Sie im Handbuch *Einführung*.

VGA

Der Anschluss für einen externen Monitor, oder VGA-Anschluss, ist eine Analogschnittstelle für ein Anzeigegerät, über die Sie ein externes VGA-Anzeigegerät, z. B. einen externen VGA-Monitor oder einen VGA-Projektor, mit dem Computer verbinden können.

▲ Um ein VGA-Anzeigegerät anzuschließen, schließen Sie das Kabel des Anzeigegeräts an den Anschluss für einen externen Monitor an.



HINWEIS: Produktspezifische Anleitungen zum Umschalten der Bildschirmanzeige finden Sie im Handbuch *Einführung*.

HDMI

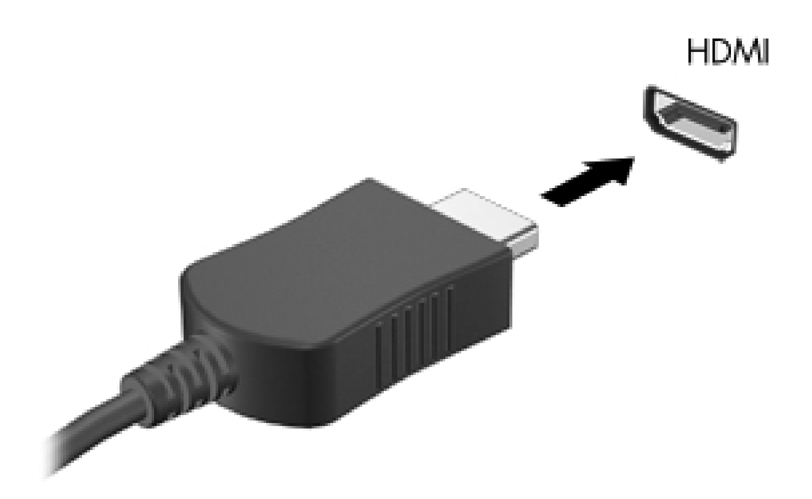
Über diesen Anschluss können ein optionales Anzeige- oder Audiogerät (z. B. ein High-Definition-Fernsehgerät) oder andere kompatible digitale Geräte oder Audiokomponenten an den Computer angeschlossen werden.

HINWEIS: Um Videosignale über den HDMI-Anschluss zu übertragen, benötigen Sie ein HDMI-Kabel (separat zu erwerben).

Es kann ein HDMI-Gerät an den HDMI-Anschluss am Computer angeschlossen werden. Die auf dem Computerdisplay angezeigten Informationen können gleichzeitig auf dem HDMI-Gerät angezeigt werden.

So schließen Sie ein Video- oder Audiogerät an den HDMI-Anschluss an:

1. Verbinden Sie ein Ende des HDMI-Kabels mit dem HDMI-Anschluss am Computer.



2. Schließen Sie das andere Ende des Kabels am Videogerät an. Weitere Informationen finden Sie in der Bedienungsanleitung des Geräteherstellers.

HINWEIS: Produktspezifische Anleitungen zum Umschalten der Bildschirmanzeige finden Sie im Handbuch *Einführung*.

Konfigurieren der Audiofunktionen für HDMI

Zum Konfigurieren der HDMI-Audiofunktion schließen Sie zunächst ein Audio- oder Videogerät, wie z. B. ein High-Definition-Fernsehgerät, an den HDMI-Anschluss am Computer an. Konfigurieren Sie anschließend das Standard-Audiowiedergabegerät wie folgt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für **Lautsprecher** im Infobereich außen rechts in der Taskleiste, und klicken Sie dann auf **Wiedergabegeräte**.
2. Klicken Sie in der Registerkarte „Wiedergabe“ entweder auf **Digitaler Ausgang** oder **Digitales Ausgabegerät (HDMI)**.
3. Klicken Sie auf **Als Standard** und anschließend auf **OK**.

So schalten Sie die Audiofunktion der Computerlautsprecher wieder ein:

1. Klicken Sie mit der rechten Maustaste auf das Symbol für **Lautsprecher** im Infobereich außen rechts in der Taskleiste, und klicken Sie dann auf **Wiedergabegeräte**.
2. Klicken Sie auf der Registerkarte „Wiedergabe“ auf **Lautsprecher**.
3. Klicken Sie auf **Als Standard** und anschließend auf **OK**.

Intel Wireless Display (bestimmte Modelle)

Mit Intel® Wireless Display können Sie Ihren Computerinhalt ohne Kabel für Ihren Fernseher freigeben. Für ein Wireless-Display benötigen Sie einen Wireless-TV-Adapter, der separat erworben werden muss. Inhalte, die einen Ausgabeschutz aufweisen, wie beispielsweise DVD- und Blu-ray-Discs, können nicht über das Intel Wireless Display wiedergegeben werden. Nähere Informationen über die Verwendung des Wireless-TV-Adapters finden Sie in den Anleitungen des Geräteherstellers.

HINWEIS: Stellen Sie sicher, dass das Wireless-Gerät Ihres Computers aktiviert ist, bevor Sie das Wireless-Display verwenden.

4 Energieverwaltung

HINWEIS: Der Computer verfügt möglicherweise über eine Betriebstaste oder einen Netzschalter. Der Begriff *Betriebstaste* wird in diesem Handbuch für beide Bedienelemente verwendet.

Ausschalten des Computers

ACHTUNG: Nicht gespeicherte Daten gehen verloren, wenn der Computer ausgeschaltet wird.

Mit dem Befehl **Herunterfahren** werden alle geöffneten Programme einschließlich des Betriebssystems geschlossen und Display und Computer ausgeschaltet.

Fahren Sie den Computer in den folgenden Situationen herunter:

- Wenn Sie den Akku auswechseln oder auf Komponenten im Computer zugreifen müssen
- Wenn Sie ein externes Gerät anschließen, das sich nicht mit einem USB-Anschluss (Universal Serial Bus) verbinden lässt
- Wenn der Computer längere Zeit nicht benutzt wird und an keine externe Stromquelle angeschlossen ist

Sie können den Computer zwar auch mit der Betriebstaste ausschalten, es empfiehlt sich jedoch, den Windows Befehl zum Herunterfahren zu verwenden:

HINWEIS: Befindet sich der Computer im Energiesparmodus oder im Ruhezustand, müssen Sie diesen Modus zunächst beenden, bevor das System heruntergefahren werden kann.

1. Speichern Sie Ihre Daten, und schließen Sie alle offenen Programme.
2. **Windows 7** – Wählen Sie **Start > Herunterfahren**.

   Windows Vista — Wählen Sie **Start**, klicken Sie auf den Pfeil neben der Sperren-Schaltfläche und anschließend auf **Herunterfahren**.

   HINWEIS: Wenn Sie bei einer Netzwerkdomäne registriert sind, trägt die Schaltfläche die Bezeichnung „Herunterfahren“ anstelle von „Computer ausschalten“.

Wenn der Computer nicht reagiert und Sie daher nicht mit den obengenannten Methoden herunterfahren können, versuchen Sie es mit den folgenden Notabschaltverfahren in der angegebenen Reihenfolge:

- Drücken Sie die Tastenkombination strg+alt+entf, und klicken Sie dann auf die **Netzschalter**-Schaltfläche.
- Halten Sie die Betriebstaste mindestens 5 Sekunden lang gedrückt.
- Trennen Sie den Computer von der externen Stromquelle, und entfernen Sie den Akku.

Einstellen der Energieoptionen

Verwenden von Energiesparmodi

Der Computer verfügt über zwei Energiesparfunktionen, die werksseitig aktiviert sind: Energiesparmodus und Ruhezustand.

Wenn Sie den Energiesparmodus einleiten, blinken die Betriebsanzeigen, und auf dem Display wird nichts mehr angezeigt. Ihre Daten werden im Arbeitsspeicher abgelegt, wodurch sich der Energiesparmodus schneller beenden lässt als der Ruhezustand. Wenn sich der Computer für längere Zeit im Energiesparmodus befindet oder im Energiesparmodus ein kritischer Akkuladestand erreicht wird, leitet das System den Ruhezustand ein.

Beim Einleiten des Ruhezustands werden Ihre Daten auf der Festplatte in einer Ruhezustandsdatei gespeichert, und der Computer wird ausgeschaltet.

ACHTUNG: Um das Risiko einer Verschlechterung der Bild- und Audiowiedergabe, eines Verlusts der Wiedergabefunktion für Audio- und Videodaten und eines Datenverlusts zu verringern, sollten Sie während des Lesens oder Beschreibens einer Disc oder einer externen Speicherkarte nicht den Energiesparmodus oder Ruhezustand einleiten.

HINWEIS: Solange sich der Computer im Energiesparmodus oder Ruhezustand befindet, kann keinerlei Netzwerkverbindung eingeleitet und keine Computerfunktion genutzt werden.

Einleiten und Beenden des Energiesparmodus

Das System leitet standardmäßig bei Akkubetrieb oder bei externer Stromversorgung nach einer bestimmten Zeitspanne ohne Aktivität den Energiesparmodus ein.

Die Energieeinstellungen und Zeitlimits können im Fenster **Energieoptionen** in der Windows Systemsteuerung geändert werden.

Wenn der Computer eingeschaltet ist, können Sie den Energiesparmodus auf folgende Weise aktivieren:

- Drücken Sie kurz die Betriebstaste.
- Schließen Sie das Display.
- **Windows 7** – Wählen Sie **Start**, klicken Sie auf den Pfeil neben der Schaltfläche zum Herunterfahren und anschließend auf **Energie sparen**.

  Windows Vista – Wählen Sie **Start**, klicken Sie auf den Pfeil neben der Sperren-Schaltfläche und anschließend auf **Energie sparen**.

So beenden Sie den Energiesparmodus:

- Drücken Sie kurz die Betriebstaste.
- Wenn das Display geschlossen ist, öffnen Sie es.
- Drücken Sie eine Taste auf der Tastatur.
- Tippen Sie auf oder bewegen Sie den Finger über das TouchPad.

Wenn der Computer den Energiesparmodus beendet, leuchten die Betriebsanzeigen und die Bildschirmanzeige, bei der Ihre Arbeit unterbrochen wurde, wird wiederhergestellt.

HINWEIS: Wenn Sie den Kennwortschutz für das Beenden des Energiesparmodus eingerichtet haben, müssen Sie Ihr Windows Kennwort eingeben, bevor Sie fortfahren können.

Einleiten und Beenden des Ruhezustands

Das System leitet standardmäßig bei Akkubetrieb oder externer Stromversorgung, oder wenn ein kritischer Akkuladestand erreicht wird, nach einer bestimmten Zeitspanne ohne Aktivität automatisch den Ruhezustand ein.

Die Energieeinstellungen und Zeitlimits können in der Windows Systemsteuerung geändert werden.

So leiten Sie den Ruhezustand ein:

▲ **Windows 7** – Wählen Sie **Start**, klicken Sie auf den Pfeil neben der Schaltfläche zum Herunterfahren und anschließend auf **Ruhezustand**.

Windows Vista – Wählen Sie **Start**, klicken Sie auf den Pfeil neben der Sperren-Schaltfläche und anschließend auf **Ruhezustand**.

So beenden Sie den Ruhezustand:

▲ Drücken Sie kurz die Betriebstaste.

Die Betriebsanzeigen leuchten und die Bildschirmanzeige, bei der Ihre Arbeit unterbrochen wurde, wird wiederhergestellt.

HINWEIS: Wenn Sie den Kennwortschutz für das Beenden des Ruhezustands eingerichtet haben, müssen Sie Ihr Windows Kennwort eingeben, bevor Sie fortfahren können.

Verwenden der Energieanzeige

Das Symbol für die Energieanzeige befindet sich im Infobereich rechts außen in der Taskleiste. Über die Energieanzeige haben Sie schnell Zugriff auf die Energieeinstellungen und können den aktuellen Akkuladestand anzeigen.

- Bewegen Sie den Mauszeiger über das Symbol für die Energieanzeige, um den Prozentwert der verbleibenden Akkuladung und den aktuellen Energiesparplan anzuzeigen.
- Um auf die Energieoptionen zuzugreifen oder das Energieschema zu ändern, klicken Sie auf das Symbol für die Energieanzeige, und wählen Sie eine Option aus der Liste.

Verschiedene Energieanzeigesymbole geben an, ob der Computer mit einem Akku oder über eine externe Stromquelle betrieben wird. Das Symbol zeigt zudem eine Meldung an, wenn der Akku einen niedrigen oder kritischen Akkuladestand erreicht hat.

Verwenden von Energiesparplänen

Ein Energiesparplan umfasst eine Reihe von Systemeinstellungen, die festlegen, wie der Computer Energie verbraucht. Energiesparpläne helfen Ihnen dabei, Energie zu sparen oder die Leistung zu optimieren.

Anzeigen des aktuellen Energiesparplans

Wenden Sie eine der folgenden Methoden an:

- Klicken Sie im Infobereich außen rechts in der Taskleiste auf das Symbol für die Energieanzeige.
- **Windows 7** – Wählen Sie **Start > Systemsteuerung > System und Sicherheit > Energieoptionen**.
- **Windows Vista** – Wählen Sie **Start > Systemsteuerung > System und Wartung > Energieoptionen**.

Auswählen eines anderen Energiesparplans

Wenden Sie eine der folgenden Methoden an:

- Klicken Sie auf das Symbol für die Energieanzeige im Infobereich, und wählen Sie dann einen Energiesparplan aus der Liste aus.
- **Windows 7** – Wählen Sie **Start > Systemsteuerung > System und Sicherheit > Energieoptionen**, und wählen Sie anschließend ein Element aus der Liste aus.

  Windows Vista – Wählen Sie **Start > Systemsteuerung > System und Wartung > Energieoptionen**, und wählen Sie anschließend ein Element aus der Liste aus.

Anpassen des Energiesparplans

Windows 7

1. Klicken Sie auf das Symbol für die Energieanzeige im Infobereich, und klicken Sie dann auf **Weitere Energieoptionen**.

   – ODER –

   Wählen Sie **Start > Systemsteuerung > System und Sicherheit > Energieoptionen**.
2. Wählen Sie einen Energiesparplan, und klicken Sie dann auf **Planeinstellungen ändern**.
3. Ändern Sie die Einstellungen nach Bedarf.
4. Klicken Sie auf **Erweiterte Energieeinstellungen ändern**, und nehmen Sie die gewünschten Änderungen vor.

Windows Vista

1. Klicken Sie auf das Symbol für die Energieanzeige im Infobereich, und klicken Sie dann auf **Weitere Energieoptionen**.

   – ODER –

   Wählen Sie **Start > Systemsteuerung > System und Wartung > Energieoptionen**.

2. Wählen Sie einen Energiesparplan, und klicken Sie dann auf **Planeinstellungen ändern**.
3. Ändern Sie die Einstellungen nach Bedarf.
4. Klicken Sie auf **Erweiterte Energieeinstellungen ändern**, und nehmen Sie die gewünschten Änderungen vor.

Einrichten des Kennwortschutzes für die Reaktivierung

So legen Sie fest, dass beim Beenden des Energiesparmodus oder des Ruhezustands ein Kennwort eingegeben werden muss:

Windows 7

1. Wählen Sie **Start > Systemsteuerung > System und Sicherheit > Energieoptionen**.
2. Klicken Sie im linken Fensterausschnitt auf **Kennwort ist für Reaktivierung erforderlich**.
3. Klicken Sie auf **Einige Einstellungen sind momentan nicht verfügbar**.
4. Klicken Sie auf **Kennwort ist erforderlich (empfohlen)**.

   HINWEIS: Wenn Sie ein Kennwort für Ihr Benutzerkonto erstellen oder Ihr aktuelles Kennwort ändern möchten, klicken Sie auf **Kennwort des Benutzerkontos erstellen oder ändern**, und folgen Sie den Anleitungen auf dem Bildschirm. Wenn Sie kein Kennwort für ein Benutzerkonto erstellen müssen, gehen Sie weiter zu Schritt 5.

5. Klicken Sie auf **Änderungen speichern**.

Windows Vista

1. Wählen Sie **Start > Systemsteuerung > System und Wartung > Energieoptionen**.
2. Klicken Sie im linken Fensterausschnitt auf **Kennwort ist für Reaktivierung erforderlich**.
3. Klicken Sie auf **Einige Einstellungen sind momentan nicht verfügbar**.
4. Klicken Sie auf **Kennwort ist erforderlich (empfohlen)**.
5. Klicken Sie auf **Änderungen speichern**.

Verwenden von Power Assistant (bestimmte Modelle)

Mit Power Assistant können Sie Systemeinstellungen konfigurieren, um den Stromverbrauch und die Akkunutzungsdauer Ihres Computers zu optimieren. Power Assistant stellt Tools und Informationen bereit, mit denen Sie fundierte Entscheidungen zur Energieverwaltung treffen können:

- Vorhersagen zum Stromverbrauch für angenommene Systemkonfigurationen
- Vordefinierte Energieprofile
- Einzelheiten zur Verwendung und Diagramme, die Trends im Stromverbrauch über einen bestimmten Zeitraum anzeigen

So starten Sie Power Assistant, wenn Windows ausgeführt wird:

▲ Wählen Sie **Start > Alle Programme > HP > HP Power Assistant**.

– ODER –

Drücken Sie fn-f6 (bestimmte Modelle).

Weitere Informationen zur Verwendung, Konfiguration und Verwaltung von Power Assistant finden Sie in der Hilfe zur Power Assistant Software.

Akkubetrieb

VORSICHT! Zur Vermeidung möglicher Sicherheitsrisiken verwenden Sie nur den im Lieferumfang des Computers enthaltenen Akku, einen Ersatzakku von HP oder zulässige Akkus, die als Zubehör von HP erworben wurden.

Ist der Computer nicht an eine externe Stromquelle angeschlossen, wird er mit Akkustrom betrieben. Die Akkunutzungsdauer kann unterschiedlich ausfallen. Sie hängt von den Einstellungen in der Energieverwaltung, von ausgeführten Programmen, der Helligkeit des Displays, den an den Computer angeschlossenen externen Geräten und anderen Faktoren ab. Wenn Sie den Akku im Computer belassen, wird er jedes Mal aufgeladen, wenn der Computer an eine Netzstromquelle angeschlossen ist. Außerdem sind Ihre Daten im Falle eines Stromausfalls geschützt. Wenn sich ein aufgeladener Akku im Computer befindet und der Computer mit Netzstrom versorgt wird, schaltet er automatisch auf Akkustrom um, wenn das Netzteil vom Computer getrennt wird oder der Netzstrom ausfällt.

HINWEIS: Wird der Computer von der externen Stromquelle getrennt, so wird die Helligkeit des Displays automatisch verringert, um die Akkunutzungsdauer zu verlängern. Informationen zum Erhöhen oder Verringern der Helligkeit des Displays erhalten Sie im Handbuch *Einführung*. Einige Computermodelle können zwischen verschiedenen Grafikmodi umschalten, um die Akkulebensdauer zu verlängern. Weitere Informationen finden Sie unter „Umschalten zwischen Grafikmodi (bestimmte Modelle)“ auf Seite 34.

Weitere Informationen zum Akku

Hilfe und Support bietet folgende Tools und Informationen zum Akku:

- Akku-Test, ein Tool zum Überprüfen der Akkuleistung
- Informationen zur Kalibrierung, Energieverwaltung sowie zur sachgerechten Pflege und Aufbewahrung, um die Akkunutzungsdauer zu verlängern
- Informationen zu Akkutypen, technischen Daten, Nutzungsdauer und Kapazität

So greifen Sie auf die Akkuinformationen zu:

▲ Wählen Sie **Start > Hilfe und Support > Lernmöglichkeiten > Energiesparpläne: Häufig gestellte Fragen**.

Verwenden von Akku-Test

Akku-Test in Hilfe und Support liefert Informationen über den Status des Akkus im Computer.

So führen Sie Akku-Test aus:

1. Schließen Sie das Netzteil an den Computer an.

   HINWEIS: Für eine korrekte Funktionsweise von Akku-Test muss der Computer an eine externe Stromquelle angeschlossen sein.

2. Wählen Sie **Start > Hilfe und Support > Problembehandlung > Stromversorgung, Wärmemanagement und mechanische Komponenten**.

3. Klicken Sie auf die Registerkarte **Stromversorgung** und anschließend auf **Akku-Test**.

Akku-Test prüft den Akku und seine Zellen, um festzustellen, ob sie fehlerfrei funktionieren. Anschließend werden die Ergebnisse als Bericht ausgegeben.

Anzeigen des Akkuladestands

▲ Bewegen Sie den Mauszeiger über das Symbol für die Energieanzeige, das sich im Infobereich ganz rechts in der Taskleiste befindet.

Maximieren der Akkunutzungsdauer

Die Akkunutzungsdauer ist abhängig von den Funktionen, die Sie während des Akkubetriebs verwenden. Die Nutzungsdauer wird mit der Zeit kürzer, da die Akkukapazität nachlässt.

Tipps zum Maximieren der Akkunutzungsdauer:

- Verringern Sie die Helligkeit für die Displayanzeige.
- Nehmen Sie den Akku aus dem Computer, wenn er nicht benötigt oder geladen wird.
- Bewahren Sie den Akku kühl und trocken auf.
- Wählen Sie **Energiesparmodus** im Fenster „Energieoptionen“.

Niedriger Akkuladestand

In diesem Abschnitt werden die Alarmfunktionen und Systemreaktionen beschrieben, die werksseitig eingestellt sind. Einige Alarmfunktionen des Low-Battery-Modus und Systemreaktionen bei einem niedrigen Akkuladestand können über die **Energieoptionen** der Windows Systemsteuerung geändert werden. Die Einstellungen im Fenster **Energieoptionen** wirken sich nicht auf die LEDs aus.

Feststellen eines niedrigen Akkuladestands

Wenn ein Akku als einzige Stromquelle des Computers verwendet wird und der Ladestand des Akkus niedrig oder kritisch ist, reagiert der Computer folgendermaßen:

- Die Akkuanzeige (bestimmte Modelle) weist auf einen niedrigen oder kritischen Akkuladestand hin.

  HINWEIS: Weitere Informationen zur Akkuanzeige erhalten Sie im Handbuch *Einführung*.

– ODER –

- Das Symbol für die Energieanzeige im Infobereich zeigt bei niedrigem oder kritischem Akkuladestand eine entsprechende Meldung an.

HINWEIS: Weitere Informationen zur Energieanzeige finden Sie unter „Verwenden der Energieanzeige“ auf Seite 25.

Auf einen kritischen Akkuladestand reagiert der Computer auf folgende Weise:

- Wenn der Ruhezustand aktiviert und der Computer eingeschaltet ist oder sich im Energiesparmodus befindet, wechselt der Computer in den Ruhezustand.
- Wenn der Ruhezustand deaktiviert und der Computer eingeschaltet ist oder sich im Energiesparmodus befindet, bleibt er kurz im Energiesparmodus und schaltet dann ab, wobei alle nicht gespeicherten Daten verloren gehen.

Beheben eines niedrigen Akkuladestands

Beheben eines niedrigen Akkuladestands, wenn eine externe Stromquelle vorhanden ist

▲ Schließen Sie eines der folgenden Geräte an:

  - Netzteil
  - Optionales Docking- oder Erweiterungsgerät
  - Optionales Netzteil, das als Zubehör von HP erworben wurde

Beheben eines niedrigen Akkuladestands, wenn ein aufgeladener Akku verfügbar ist

1. Schalten Sie den Computer aus, oder leiten Sie den Ruhezustand ein.
2. Ersetzen Sie den entladenen Akku durch einen aufgeladenen Akku.
3. Schalten Sie den Computer ein.

Beheben eines niedrigen Akkuladestands, wenn keine Stromquelle verfügbar ist

- Leiten Sie den Ruhezustand ein.
- Speichern Sie Ihre Arbeit, und fahren Sie den Computer herunter.

Beheben eines niedrigen Akkuladestands, wenn der Computer den Ruhezustand nicht beenden kann

Wenn die Stromversorgung des Computers nicht mehr ausreicht, um den Ruhezustand zu beenden, führen Sie die folgenden Schritte aus:

1. Ersetzen Sie den entladenen Akku durch einen aufgeladenen Akku, oder schließen Sie das Netzteil an den Computer und eine externe Stromquelle an.
2. Drücken Sie die Betriebstaste, um den Ruhezustand zu beenden.

Einsparen von Akkuenergie

- Wählen Sie unter **Energieoptionen** in der Systemsteuerung die Einstellungen für niedrigen Stromverbrauch aus.
- Deaktivieren Sie Wireless und LAN-Verbindungen, und schließen Sie alle Modemanwendungen, wenn Sie diese nicht verwenden.
- Trennen Sie alle nicht verwendeten externen Geräte, die nicht an eine externe Stromquelle angeschlossen sind.
- Beenden Sie die Wiedergabe aller nicht verwendeten externen Speicher- und Erweiterungskarten, deaktivieren oder entnehmen Sie sie.
- Verringern Sie die Displayhelligkeit.
- Leiten Sie vor einer Unterbrechung der Arbeit den Energiesparmodus oder den Ruhezustand ein, oder schalten Sie den Computer aus.

Aufbewahren von Akkus

ACHTUNG: Um das Risiko einer Beschädigung des Akkus zu verringern, dürfen Sie ihn niemals längere Zeit hohen Temperaturen aussetzen.

Nehmen Sie den Akku aus dem Computer, und bewahren Sie ihn separat auf, wenn der Computer länger als zwei Wochen nicht benutzt wird und an keine externe Stromquelle angeschlossen ist.

Lagern Sie einen Akku an einem kühlen, trockenen Ort, damit er sich nicht frühzeitig entlädt.

HINWEIS: Überprüfen Sie gelagerte Akkus alle sechs Monate. Wenn der Ladestand weniger als 50 % beträgt, laden Sie den Akku vor der weiteren Lagerung auf.

Kalibrieren Sie einen Akku, der einen Monat oder länger aufbewahrt wurde, bevor Sie ihn verwenden.

Entsorgen eines gebrauchten Akkus

VORSICHT! Nehmen Sie den Akku nicht auseinander, vermeiden Sie mechanische Beschädigungen jeglicher Art, schließen Sie die Kontakte eines Akkus nicht kurz, und setzen Sie den Akku nicht Feuer oder Feuchtigkeitseinwirkung aus, um Brände, Verätzungen oder Verbrennungen zu vermeiden.

Informationen zur korrekten Entsorgung von Akkus finden Sie im Dokument *Hinweise zu Zulassung, Sicherheit und Umweltverträglichkeit*.

Austauschen des Akkus

In Windows 7 werden Sie von Akku-Test, das unter Hilfe und Support aufgerufen werden kann, darauf aufmerksam gemacht, dass der Akku ersetzt werden sollte, wenn eine interne Zelle nicht korrekt geladen wird oder die Akkuladekapazität nur noch gering ist. Wenn für den Akku unter Umständen noch eine HP Garantie gilt, enthalten die Anleitungen eine Garantie-ID. Eine Meldung verweist Sie auf die HP Website, auf der Sie weitere Informationen zum Bestellen eines Ersatzakkus erhalten.

Anschließen an die externe Netzstromversorgung

HINWEIS: Informationen zum Anschließen an den Netzstrom finden Sie auf dem Poster *Installationsanleitungen*, das im Lieferumfang des Computers enthalten ist.

Die externe Netzstromversorgung erfolgt durch ein zugelassenes Netzteil oder ein optionales Docking- oder Erweiterungsgerät.

VORSICHT! Um mögliche Sicherheitsrisiken zu vermeiden, darf nur das mit dem Computer gelieferte Netzteil, ein von HP bereitgestelltes Ersatznetzteil oder ein von HP erworbenes Netzteil verwendet werden.

Schließen Sie den Computer in den folgenden Situationen an das Stromnetz an:

VORSICHT! Laden Sie den Akku des Computers nicht an Bord von Flugzeugen auf.

- Beim Aufladen oder Kalibrieren eines Akkus
- Beim Installieren oder Aktualisieren von Systemsoftware
- Beim Schreiben von Daten auf eine CD, DVD oder BD (bestimmte Modelle)
- Beim Durchführen der Defragmentierung
- Beim Sichern oder Wiederherstellen des Systems

Beim Anschließen des Computers an das Stromnetz geschieht Folgendes:

- Der Akku wird aufgeladen.
- Ist der Computer eingeschaltet, so verändert sich die Energieanzeige im Infobereich.

Beim Trennen des Computers von der Stromversorgung geschieht Folgendes:

- Der Computer schaltet auf den Betrieb mit Akkustrom um.
- Die Helligkeit des Displays wird automatisch verringert, um die Akkunutzungsdauer zu verlängern.

Testen eines Netzteils

Testen Sie das Netzteil, wenn der Computer bei Netzstromversorgung eines der folgenden Symptome aufweist:

- Der Computer lässt sich nicht einschalten.
- Auf dem Display wird nichts angezeigt.
- Die Betriebsanzeigen leuchten nicht.

So testen Sie das Netzteil:

1. Schalten Sie den Computer aus.
2. Entfernen Sie den Akku aus dem Computer.
3. Verbinden Sie das Netzteil mit dem Computer, und stecken Sie es dann an einer Steckdose an.
4. Schalten Sie den Computer ein.
   - Wenn die Betriebsanzeigen l *euchten*, funktioniert das Netzteil ordnungsgemäß.
   - Wenn die Betriebsanzeigen *nicht leuchten*, ist das Netzteil defekt und muss ausgetauscht werden.

Wenden Sie sich an den HP Kundensupport, um Informationen zum Erwerb eines Ersatznetzteils zu erhalten.

Umschalten zwischen Grafikmodi (bestimmte Modelle)

Einige Computer sind mit umschaltbaren Grafikeffekten ausgestattet und verfügen über zwei Modi zur Grafikverarbeitung. Wenn Sie von Netzstrom- zu Akkubetrieb wechseln, kann der Computer vom Grafikmodus mit hoher Leistung in einen Energiesparmodus umschalten, um den Akku zu schonen. Ebenso gilt: Wenn Sie von Akku- zu Netzstrombetrieb wechseln, kann auch der Computer wieder zurück zum Grafikmodus mit hoher Leistung wechseln.

HINWEIS: Um die Leistung des Computers zu optimieren, können in einigen Fällen die Modi nicht gewechselt werden oder Sie werden zum Umschalten aufgefordert. Möglicherweise müssen Sie auch alle Programme schließen, bevor Sie umschalten können.

HINWEIS: HDMI (bestimmte Modelle) kann nur im Modus mit hoher Leistung verwendet werden. Wenn Sie den Energiesparmodus nutzen, können Sie HDMI nicht verwenden.

Wenn Sie zwischen Akku- und Netzstrombetrieb wechseln, wird eine Meldung angezeigt, dass der Computer die Grafikmodi umschaltet. Sie können dann wählen, ob Sie den bisherigen Grafikmodus weiterhin verwenden möchten. Wenn der Computer zwischen zwei Modi umschaltet, wird auf dem Display einige Sekunden lang nichts angezeigt. Nach Abschluss des Vorgangs wird im Infobereich eine Meldung angezeigt, und der Bildschirm wird wieder angezeigt.

HINWEIS: Wenn Sie zwischen den Grafikmodi wechseln, wird bei bestimmten Computermodellen, wenn diese sich im Tablet PC-Modus befinden, die Bildschirmausrichtung zurückgesetzt.

5 Externe Karten und Geräte

Verwenden von Karten für Speicherkarten-Lesegeräte (bestimmte Modelle)

Optionale digitale Karten ermöglichen eine sichere Datenspeicherung und die komfortable gemeinsame Nutzung von Daten. Diese Karten werden oft mit Kameras und Handhelds oder anderen Computern verwendet, die mit einem entsprechenden Steckplatz ausgestattet sind.

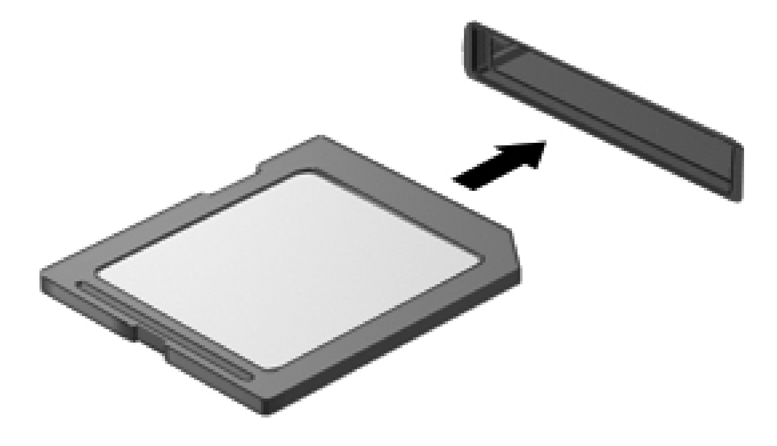
Informationen dazu, welche Formate für digitale Karten auf dem Computer unterstützt werden, finden Sie im Handbuch *Einführung*.

Einsetzen einer digitalen Karte

⚠ **ACHTUNG:** Üben Sie beim Einsetzen digitaler Karten nur minimalen Druck aus, um die Anschlüsse nicht zu beschädigen.

1. Halten Sie die Karte mit der Beschriftungsseite nach oben und dem Anschluss in Richtung Computer.

2. Setzen Sie die Karte in das Speicherkarten-Lesegerät ein, und drücken Sie die Karte nach innen, bis sie fest sitzt.

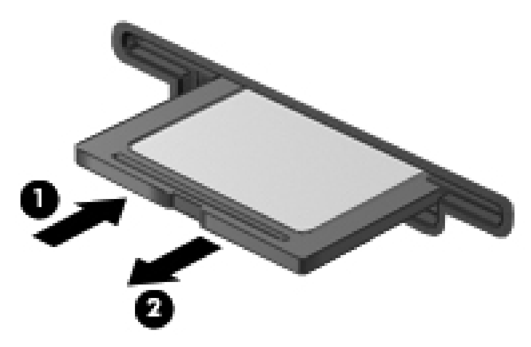


Ein akustisches Signal zeigt an, dass das Gerät erkannt wurde, und ein Menü mit Optionen wird angezeigt.

Entfernen einer digitalen Karte

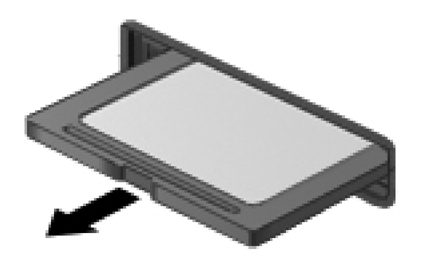
⚠ **ACHTUNG:** Zur Reduzierung des Risikos von Datenverlusten oder einer Systemblockierung gehen Sie folgendermaßen vor, um eine digitale Karte sicher herauszunehmen.

1. Speichern Sie Ihre Daten und schließen Sie alle Programme, die auf die digitale Karte zugreifen.
2. Klicken Sie im Infobereich außen rechts in der Taskleiste auf das Symbol zum Entfernen von Hardware. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.
3. Drücken Sie die Karte vorsichtig nach innen **(1)**, und nehmen Sie sie dann aus dem Steckplatz **(2)**.



– ODER –

Ziehen Sie die Karte aus dem Steckplatz.



Verwenden von PC Cards (bestimmte Modelle)

Eine PC Card ist so groß wie eine Kreditkarte und entspricht den Spezifikationen der PCMCIA (Personal Computer Memory Card International Association). Der PC Card-Steckplatz unterstützt die folgenden PC Card-Typen:

- 32-Bit (CardBus)- und 16-Bit-PC Cards
- PC Cards vom Typ I oder II

HINWEIS: Zoomed Video PC Cards und 12-V-PC Cards werden nicht unterstützt.

Konfigurieren einer PC Card

Um das Risiko zu verringern, dass andere PC Cards während der Konfiguration nicht mehr unterstützt werden, installieren Sie nur die für das Gerät erforderliche Software. Wenn Sie laut Anleitung des PC Card-Herstellers Gerätetreiber installieren sollen:

- Installieren Sie nur die Gerätetreiber für Ihr Betriebssystem.
- Installieren Sie keine weitere Software, wie zum Beispiel Card Services, Socket Services oder Aktivierungsprogramme, die vom PC Card-Hersteller geliefert werden.

Einsetzen einer PC Card

ACHTUNG: Um Schäden am Computer oder an externen Speicher- und Erweiterungskarten vorzubeugen, setzen Sie keine ExpressCard in einen PC Card-Steckplatz ein.

ACHTUNG: So verringern Sie das Risiko, dass Anschlüsse beschädigt werden:

Üben Sie beim Einsetzen einer PC Card nur minimalen Druck aus.

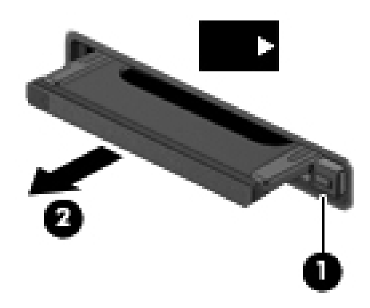
Bewegen oder transportieren Sie den Computer nicht, wenn eine PC Card gerade in Betrieb ist.

Im PC Card-Steckplatz befindet sich möglicherweise ein Schutzeinsatz. Der Einsatz muss entfernt werden, bevor eine PC Card eingesetzt werden kann:

1. Drücken Sie die Auswurftaste für die PC Card **(1)**.

   Dadurch wird die Taste so positioniert, dass durch erneutes Drücken der Schutzeinsatz freigegeben wird.

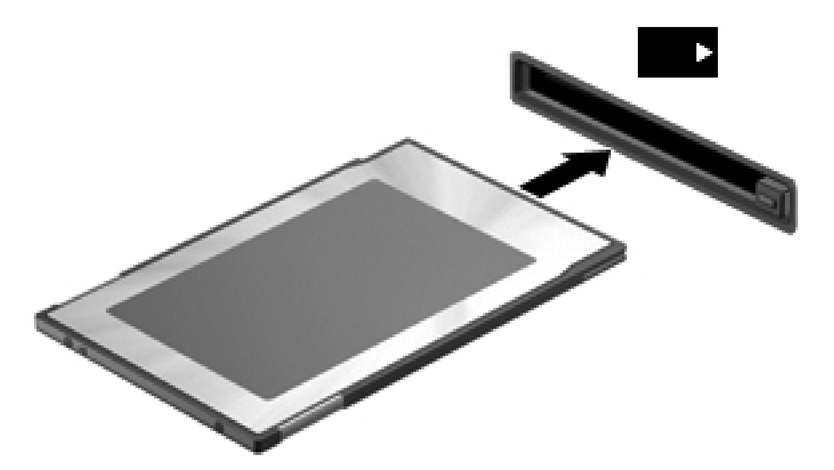
2. Drücken Sie die Auswurftaste für die PC Card erneut, um den Schutzeinsatz zu entfernen.
3. Ziehen Sie den Einsatz aus dem Steckplatz **(2)**.



So setzen Sie eine PC Card ein:

1. Halten Sie die Karte mit der Beschriftungsseite nach oben und dem Anschluss in Richtung Computer.

2. Setzen Sie die Karte in den PC Card-Steckplatz ein, und drücken Sie die Karte hinein, bis sie vollständig eingesetzt ist.



Ein akustisches Signal zeigt an, dass die Karte erkannt wurde, und u. U. wird ein Menü mit verfügbaren Optionen angezeigt.

HINWEIS: Wenn Sie eine PC Card zum ersten Mal anschließen, informiert Sie eine Meldung im Infobereich darüber, dass das Gerät vom Computer erkannt wurde.

HINWEIS: Deaktivieren oder entfernen Sie deshalb nicht verwendete PC Cards, um Energie zu sparen.

Entfernen einer PC Card

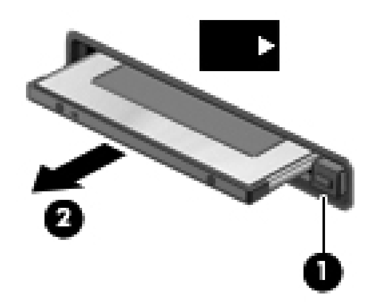
ACHTUNG: Zur Reduzierung des Risikos von Datenverlusten oder einer Systemblockierung müssen Sie die PC Card deaktivieren, bevor Sie sie herausnehmen.

1. Speichern Sie Ihre Daten, und schließen Sie alle Programme, die auf die PC Card zugreifen.
2. Klicken Sie auf das Symbol zum Entfernen von Hardware im Infobereich außen rechts in der Taskleiste, und folgen Sie den Anleitungen auf dem Bildschirm.
3. Geben Sie die PC Card frei, und entnehmen Sie sie:
   a. Drücken Sie die Auswurftaste für die PC Card **(1)**.

      Dadurch wird die Taste so positioniert, dass durch erneutes Drücken die PC Card freigegeben wird.

   b. Drücken Sie die Auswurftaste für die PC Card erneut, um die PC Card zu entfernen.

   c. Ziehen Sie die PC Card aus dem Steckplatz **(2)**.



Verwenden von ExpressCards (bestimmte Modelle)

Bei einer ExpressCard handelt es sich um eine Hochleistungs-PC Card, die in den ExpressCard-Steckplatz eingesetzt wird.

Wie Standard-PC Cards sind auch ExpressCards so konstruiert, dass sie den Standardspezifikationen der PCMCIA entsprechen.

Konfigurieren einer ExpressCard

Installieren Sie nur die für die Karte erforderliche Software. Wenn Sie der Hersteller der ExpressCard zur Installation kartenspezifischer Treiber auffordert, gehen Sie wie folgt vor:

- Installieren Sie nur die Gerätetreiber für Ihr Betriebssystem.
- Installieren Sie keine zusätzliche Software, wie zum Beispiel Card Services, Socket Services oder Aktivierungsprogramme, die vom ExpressCard-Hersteller bereitgestellt werden.

Einsetzen einer ExpressCard

ACHTUNG: Um Schäden am Computer oder an externen Speicher- und Erweiterungskarten vorzubeugen, setzen Sie keine PC Card in einen ExpressCard-Steckplatz ein.

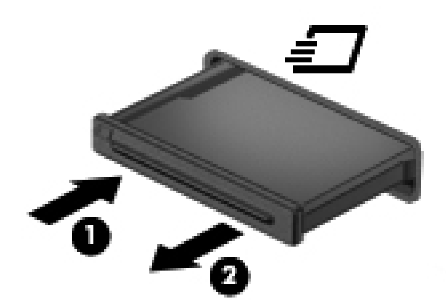
ACHTUNG: So verringern Sie das Risiko, dass Anschlüsse beschädigt werden:

Üben Sie beim Einsetzen einer ExpressCard nur minimalen Druck aus.

Bewegen oder transportieren Sie den Computer nicht, wenn eine ExpressCard gerade in Betrieb ist.

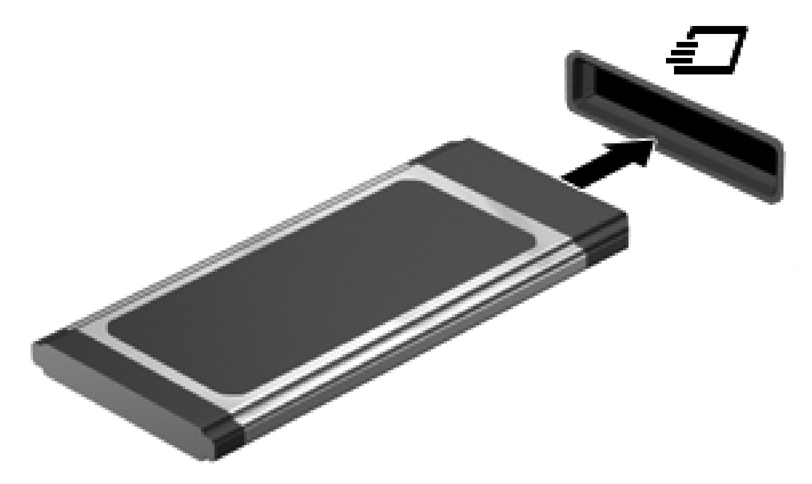
Im ExpressCard-Steckplatz befindet sich möglicherweise ein Schutzeinsatz. So entfernen Sie den Einsatz:

1. Drücken Sie den Einsatz nach innen **(1)**, um ihn freizugeben.
2. Ziehen Sie den Einsatz aus dem Steckplatz **(2)**.



So setzen Sie eine ExpressCard ein:

1. Halten Sie die Karte mit der Beschriftungsseite nach oben und dem Anschluss in Richtung Computer.
2. Setzen Sie die Karte in den ExpressCard-Steckplatz ein, und drücken Sie die Karte hinein, bis sie vollständig eingesetzt ist.



Ein akustisches Signal zeigt an, dass die Karte erkannt wurde, und u. U. wird ein Menü mit Optionen angezeigt.

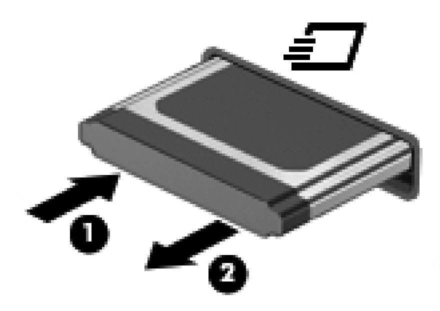
HINWEIS: Wenn Sie eine ExpressCard zum ersten Mal anschließen, informiert Sie eine Meldung im Infobereich darüber, dass die Karte vom Computer erkannt wurde.

HINWEIS: Deaktivieren oder entfernen Sie nicht verwendete ExpressCards, um Energie zu sparen.

Entnehmen einer ExpressCard

ACHTUNG: Zur Reduzierung des Risikos von Datenverlusten oder einer Systemblockierung gehen Sie folgendermaßen vor, um eine ExpressCard sicher herauszunehmen.

1. Speichern Sie Ihre Daten, und schließen Sie alle Programme, die auf die ExpressCard zugreifen.
2. Klicken Sie auf das Symbol zum Entfernen von Hardware im Infobereich außen rechts in der Taskleiste, und folgen Sie den Anleitungen auf dem Bildschirm.
3. Geben Sie die ExpressCard frei, und entfernen Sie sie:
   a. Drücken Sie die ExpressCard sanft nach innen **(1)**, damit sie freigegeben wird.
   b. Ziehen Sie die ExpressCard aus dem Steckplatz **(2)**.



Verwenden von Smart Cards (bestimmte Modelle)

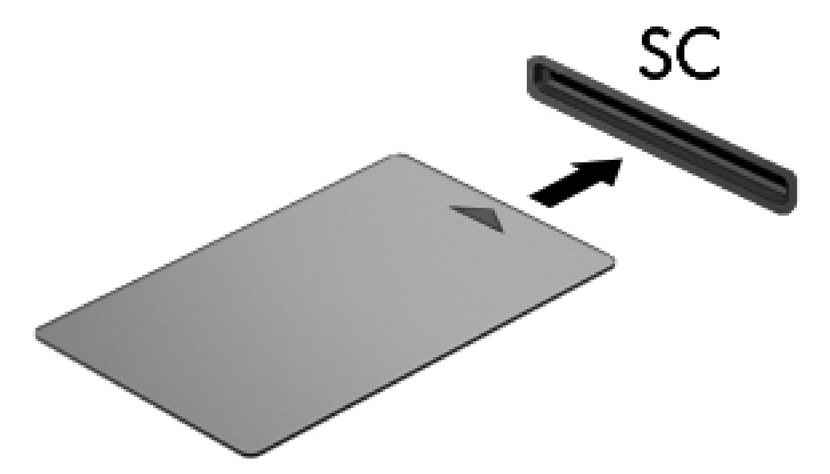
HINWEIS: Der Begriff *Smart Card* in diesem Kapitel wird sowohl für Smart Cards als auch für Java™ Cards verwendet.

Eine Smart Card hat die Größe einer Kreditkarte und enthält einen Mikrochip zum Speichern von Daten sowie einen Mikroprozessor. Smart Cards verfügen wie PCs über ein Betriebssystem, um die Eingabe und Ausgabe von Daten zu verwalten. Sie beinhalten darüber hinaus Sicherheitsfunktionen, die vor Missbrauch schützen sollen. Handelsübliche Smart Cards werden mit einem Smart Card-Lesegerät verwendet (bestimmte Modelle).

Eine PIN ist erforderlich, um auf die Daten auf dem Mikrochip zuzugreifen. Weitere Informationen zu den Sicherheitsfunktionen der Smart Card finden Sie unter Hilfe und Support.

Einsetzen einer Smart Card

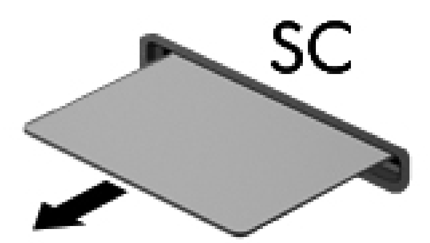
1. Schieben Sie die Smart Card mit der Beschriftungsseite nach oben vorsichtig in das Lesegerät für Smart Cards, bis sie vollständig eingesetzt ist.



2. Folgen Sie den Anleitungen auf dem Bildschirm, um sich mit der Smart Card-PIN beim Computer anzumelden.

Entfernen einer Smart Card

▲ Fassen Sie die Kante der Smart Card, und ziehen Sie sie aus dem Lesegerät für Smart Cards heraus.



Verwenden eines USB-Geräts

USB (Universal Serial Bus) ist eine Hardwareschnittstelle, mit der Sie optionale externe USB-Geräte (wie beispielsweise Tastatur, Maus, Laufwerk, Drucker, Scanner oder Hub) an den Computer anschließen können.

Für einige USB-Geräte wird eventuell zusätzliche Software benötigt, die normalerweise zum Lieferumfang des Geräts gehört. Weitere Informationen über gerätespezifische Software finden Sie in den Anleitungen vom Hersteller. Diese Anleitungen werden häufig mit der Software geliefert oder auf einer Disc bzw. auf der Website des Herstellers zur Verfügung gestellt.

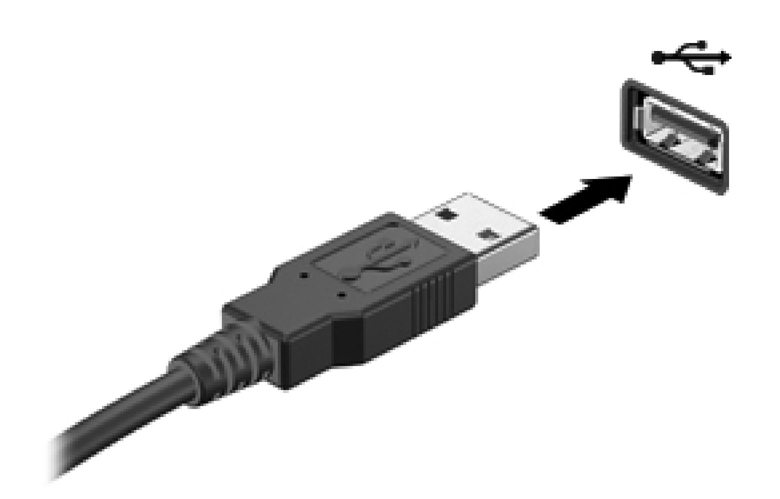
Der Computer verfügt über mindestens 1 USB-Anschluss, der USB 1.0-, USB 1.1-, USB 2.0- oder USB 3.0-Geräte unterstützt. Der Computer verfügt möglicherweise auch über einen USB-Anschluss mit Stromversorgung, der ein externes Gerät mit Strom versorgen kann, wenn ein entsprechendes USB-Kabel mit Stromversorgung verwendet wird. Ein optionales Dockinggerät bzw. ein optionaler USB-Hub besitzt weitere USB-Anschlüsse, die mit dem Computer verwendet werden können.

Anschließen eines USB-Geräts

ACHTUNG: Üben Sie beim Anschließen des Geräts nur minimalen Druck aus, um das Risiko einer Beschädigung des USB-Anschlusses zu minimieren.

▲ Schließen Sie das USB-Kabel des Geräts an den USB-Anschluss an.

HINWEIS: Möglicherweise unterscheidet sich Ihr Computer optisch leicht von den Abbildungen in diesem Handbuch.



Ein akustisches Signal zeigt an, dass das Gerät erkannt wurde.

HINWEIS: Wenn Sie ein USB-Gerät zum ersten Mal anschließen, informiert Sie eine Meldung im Infobereich darüber, dass das Gerät vom Computer erkannt wurde.

Entfernen eines USB-Geräts

ACHTUNG: Ziehen Sie nicht am Kabel, um USB-Geräte vom Computer zu trennen, da sonst die USB-Anschlüsse beschädigt werden könnten.

ACHTUNG: Zur Verringerung des Risikos von Datenverlusten oder einer Systemblockierung gehen Sie folgendermaßen vor, um das USB-Gerät sicher zu entfernen.

1. Um ein USB-Gerät zu entfernen, speichern Sie Ihre Daten, und schließen Sie alle Programme, die auf das Gerät zugreifen.
2. Klicken Sie auf das Symbol zum Entfernen von Hardware im Infobereich außen rechts in der Taskleiste, und folgen Sie den Anleitungen auf dem Bildschirm.
3. Entfernen Sie das Gerät.

Verwenden von 1394-Geräten (bestimmte Modelle)

IEEE 1394 bezeichnet eine Hardwareschnittstelle, an die Multimedia- oder Datenspeichergeräte für schnellen Datenaustausch angeschlossen werden können. Für Scanner, Digitalkameras und digitale Camcorder wird häufig ein 1394-Anschluss benötigt.

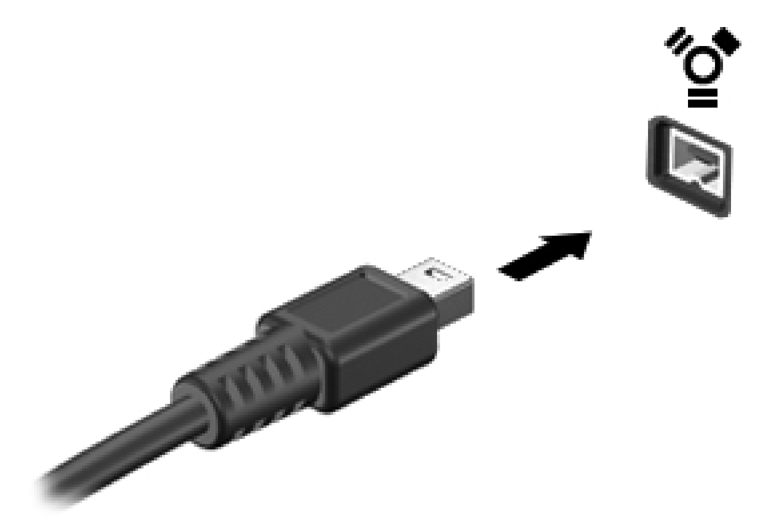
Für einige 1394-Geräte wird eventuell zusätzliche Software benötigt, die normalerweise zum Lieferumfang des Geräts gehört. Weitere Informationen zu gerätespezifischer Software finden Sie in der Bedienungsanleitung des Geräteherstellers.

Der 1394-Anschluss unterstützt auch IEEE-1394a-Geräte.

Anschließen eines 1394-Geräts

⚠ **ACHTUNG:** Üben Sie beim Anschließen des Geräts nur minimalen Druck aus, um das Risiko einer Beschädigung des 1394-Anschlusses zu minimieren.

▲ Um ein 1394-Gerät mit dem Computer zu verbinden, schließen Sie das 1394-Kabel des Geräts am 1394-Anschluss an.



Ein akustisches Signal zeigt an, dass das Gerät erkannt wurde.

Entfernen eines 1394-Geräts

⚠ **ACHTUNG:** Zur Verringerung des Risikos von Datenverlusten oder einer Systemblockierung müssen Sie das 1394-Gerät deaktivieren, bevor Sie es herausnehmen.

ACHTUNG: Ziehen Sie nicht am Kabel, um 1394-Geräte vom Computer zu trennen, da sonst die 1394-Anschlüsse beschädigt werden könnten.

1. Um ein 1394-Gerät zu entfernen, speichern Sie Ihre Daten, und schließen Sie alle Programme, die auf das Gerät zugreifen.
2. Klicken Sie auf das Symbol zum Entfernen von Hardware im Infobereich außen rechts in der Taskleiste, und folgen Sie den Anleitungen auf dem Bildschirm.
3. Entfernen Sie das Gerät.

Verwenden eines eSATA-Geräts (bestimmte Modelle)

An einen eSATA-Anschluss kann eine optionale eSATA-Hochleistungskomponente angeschlossen werden, beispielsweise eine (externe) eSATA-Festplatte.

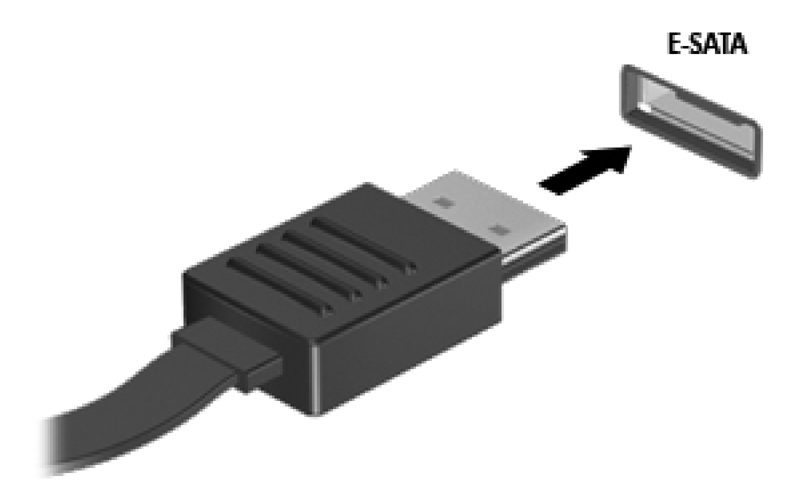
Für einige eSATA-Geräte wird eventuell zusätzliche Software benötigt, die normalerweise zum Lieferumfang des Geräts gehört. Weitere Informationen über gerätespezifische Software finden Sie in den Anleitungen des Herstellers.

HINWEIS: Der eSATA-Anschluss unterstützt auch ein optionales USB-Gerät.

Anschließen eines eSATA-Geräts

⚠ **ACHTUNG:** Üben Sie beim Anschließen des Geräts nur minimalen Druck aus, um das Risiko einer Beschädigung des eSATA-Anschlusses zu minimieren.

▲ Um ein eSATA-Gerät am Computer anzuschließen, schließen Sie das eSATA-Kabel des Geräts am eSATA-Anschluss an.



Wenn das Gerät erkannt wurde, ertönt ein akustisches Signal.

Entfernen eines eSATA-Geräts

⚠ **ACHTUNG:** Ziehen Sie nicht am Kabel, um eSATA-Geräte vom Computer zu trennen, da sonst die eSATA-Anschlüsse beschädigt werden könnten.

ACHTUNG: Zur Verringerung des Risikos von Datenverlusten oder einer Systemblockierung gehen Sie folgendermaßen vor, um das Gerät sicher zu entfernen.

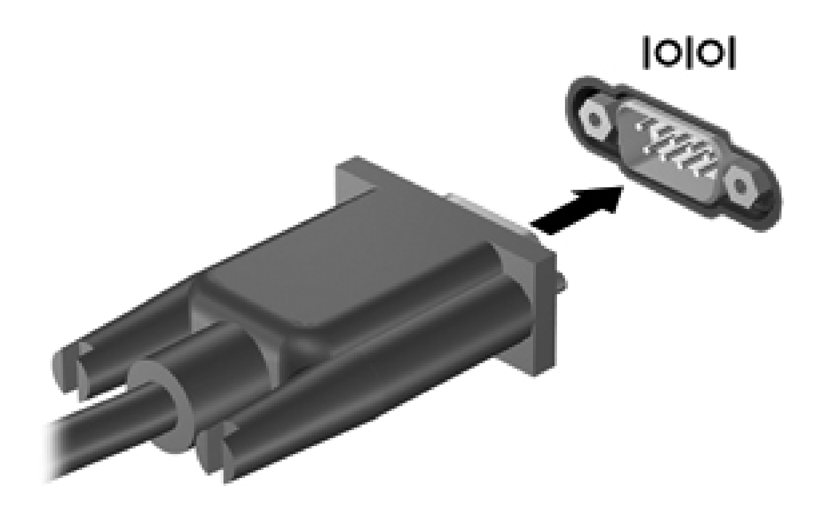
1. Um ein eSATA-Gerät zu entfernen, speichern Sie Ihre Daten, und schließen Sie alle Programme, die auf das Gerät zugreifen.
2. Klicken Sie auf das Symbol zum Entfernen von Hardware im Infobereich außen rechts in der Taskleiste, und folgen Sie den Anleitungen auf dem Bildschirm.
3. Entfernen Sie das Gerät.

Verwenden eines seriellen Geräts (bestimmte Modelle)

Bestimmte Computermodelle sind mit einem seriellen Anschluss ausgestattet, an den optionale Geräte, wie z. B. ein serielles Modem, eine Maus oder ein Drucker, angeschlossen werden können.

Für einige serielle Geräte wird eventuell zusätzliche Software benötigt, die normalerweise zum Lieferumfang des Geräts gehört. Weitere Informationen zu gerätespezifischer Software finden Sie in der Bedienungsanleitung des Geräteherstellers.

▲ Um ein serielles Gerät anzuschließen, schließen Sie das USB-Kabel am seriellen Anschluss des Computers an.



Verwenden optionaler externer Geräte

HINWEIS: Weitere Informationen über erforderliche Software und Treiber sowie Hinweise zu den entsprechenden Computeranschlüssen finden Sie in den Anleitungen des Herstellers.

So schließen Sie ein externes Laufwerk an den Computer an:

ACHTUNG: Um das Risiko von Hardwareschäden beim Anschließen eines Geräts mit eigener Stromversorgung zu reduzieren, stellen Sie sicher, dass das Gerät ausgeschaltet und das Netzkabel abgezogen ist.

1. Schließen Sie das Laufwerk an den Computer an.
2. Wenn Sie ein Laufwerk mit eigener Stromversorgung anschließen, stecken Sie das Netzkabel des Laufwerks in eine geerdete Steckdose.
3. Schalten Sie das Gerät ein.

Wenn Sie ein externes Gerät ohne eigene Stromversorgung vom Computer trennen möchten, schalten Sie das Gerät aus, und trennen Sie es vom Computer. Wenn Sie ein externes Gerät mit eigener Stromversorgung vom Computer trennen möchten, schalten Sie das Gerät aus, trennen Sie es vom Computer, und ziehen Sie dann das Netzkabel aus der Steckdose.

Verwenden optionaler externer Laufwerke

Externe Wechsellaufwerke bieten zusätzliche Möglichkeiten, Daten zu speichern und auf Daten zuzugreifen. Ein USB-Laufwerk kann hinzugefügt werden, indem es an einen USB-Anschluss am Computer angeschlossen wird.

HINWEIS: Externe optische USB-Laufwerke von HP sollten über den USB-Anschluss mit Stromversorgung am Computer angeschlossen werden.

USB-Laufwerke umfassen folgende Typen:

- 1,44-Megabyte-Diskettenlaufwerk
- Festplattenmodul
- Externes optisches Laufwerk (CD, DVD und Blu-ray)
- MultiBay-Gerät

Verwenden des Erweiterungsanschlusses (bestimmte Modelle)

Der Erweiterungsanschluss verbindet den Computer mit einem optionalen Docking- oder Erweiterungsgerät, so dass zusätzliche Ports und Anschlüsse mit dem Computer verwendet werden können.



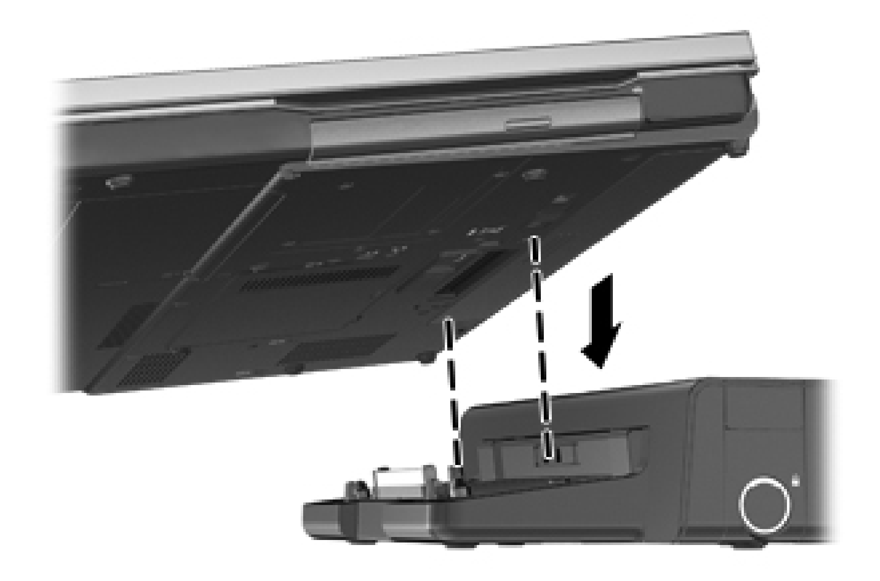
HINWEIS: Der Computer verfügt nur über einen Erweiterungsanschluss.



Verwenden des Dockinganschlusses (bestimmte Modelle)

Der Dockinganschluss verbindet den Computer mit einem optionalen Dockinggerät. Optionale Dockinggeräte besitzen weitere Anschlüsse, die zusammen mit dem Computer verwendet werden können.

HINWEIS: Möglicherweise unterscheidet sich Ihr Computer oder Dockinggerät optisch leicht von der folgenden Abbildung.



6 Laufwerke

Handhabung von Laufwerken

Laufwerke sind empfindliche Computerkomponenten, die vorsichtig behandelt werden müssen. Beachten Sie die folgenden Hinweise für den Umgang mit Laufwerken. Weitere Warnhinweise finden Sie in den jeweiligen Anleitungen.

Beachten Sie folgende Vorsichtsmaßnahmen:

- Bevor Sie einen Computer bewegen, an den eine externe Festplatte angeschlossen ist, leiten Sie den Energiesparmodus ein, und warten Sie, bis auf dem Display nichts mehr angezeigt wird, oder trennen Sie die externe Festplatte ordnungsgemäß vom Computer.
- Bevor Sie ein Laufwerk ein- oder ausbauen, müssen Sie zunächst die statische Elektrizität entladen, indem Sie die nicht lackierte Metalloberfläche des Laufwerks berühren.
- Berühren Sie nicht die Anschlusspins an einem Wechsellaufwerk oder am Computer.
- Gehen Sie vorsichtig mit Laufwerken um. Lassen Sie sie nicht fallen, und stellen Sie keine Gegenstände darauf ab.
- Schalten Sie den Computer aus, bevor Sie ein Laufwerk aus- oder einbauen. Wenn Sie sich nicht sicher sind, ob der Computer ausgeschaltet ist oder sich im Energiesparmodus oder im Ruhezustand befindet, schalten Sie ihn zunächst ein, und fahren Sie ihn dann über das Betriebssystem herunter.
- Setzen Sie ein Laufwerk nicht mit übermäßiger Kraft in einen Laufwerksschacht ein.
- Betätigen Sie die Tastatur nicht, und bewegen Sie den Computer nicht, während ein optisches Laufwerk Daten auf einen Datenträger schreibt. Der Schreibvorgang ist empfindlich gegenüber Erschütterungen.
- Wenn der Akku die einzige Stromquelle darstellt, vergewissern Sie sich, dass er ausreichend aufgeladen ist, bevor das Laufwerk auf eine Disc schreibt.
- Schützen Sie das Laufwerk vor extremen Temperaturen und Feuchtigkeit.
- Schützen Sie das Laufwerk vor Flüssigkeiten. Besprühen Sie das Laufwerk nicht mit Reinigungsmitteln.
- Nehmen Sie im Laufwerk enthaltene Medien heraus, bevor Sie das Laufwerk aus dem Laufwerksschacht entfernen, es auf Reisen mitnehmen, versenden oder lagern.

- Wenn ein Laufwerk per Post versendet werden muss, verpacken Sie es in einer Luftpolster-Versandtasche oder einer vergleichbaren Verpackung, und kennzeichnen Sie die Sendung als „Zerbrechlich“.
- Setzen Sie Laufwerke keinen Magnetfeldern aus. Sicherheitseinrichtungen mit Magnetfeldern sind z. B. Sicherheitsschleusen und Handsucher in Flughäfen. Förderbänder und ähnliche Sicherheitseinrichtungen in Flughäfen, mit denen Handgepäck kontrolliert wird, arbeiten mit Röntgenstrahlen statt mit Magnetismus und stellen daher keine Gefahr für die Laufwerke dar.

Verwenden von Festplatten

Verbessern der Festplattenleistung

Verwenden der Defragmentierung

Während Ihrer Arbeit mit dem Computer werden die Dateien auf der Festplatte fragmentiert. Bei der Defragmentierung werden die fragmentierten Dateien und Ordner auf der Festplatte wieder zusammengefügt, damit das System leistungsfähiger wird.

HINWEIS: Für Solid State-Laufwerke ist keine Laufwerksdefragmentierung erforderlich.

Sie brauchen die Defragmentierung nur zu starten, aber nicht zu überwachen. Die Defragmentierung kann je nach Größe Ihrer Festplatte und der Anzahl fragmentierter Dateien mehr als eine Stunde in Anspruch nehmen. Sie können den Vorgang nachts ausführen oder zu einer anderen Zeit, wenn Sie nicht auf den Computer zugreifen müssen.

HP empfiehlt, Ihre Festplatte mindestens einmal im Monat zu defragmentieren. Sie können die Defragmentierung so einstellen, dass sie einmal im Monat ausgeführt wird. Sie können Ihren Computer aber auch jederzeit manuell defragmentieren.

So verwenden Sie die Defragmentierung:

1. Schließen Sie den Computer an den Netzstrom an.
2. Wählen Sie **Start > Alle Programme > Zubehör > Systemprogramme > Defragmentierung**.
3. **Windows 7** – Klicken Sie auf **Datenträger defragmentieren**.

   HINWEIS: Windows verfügt über die Benutzerkontensteuerung, um die Sicherheit des Computers zu erhöhen. Sie werden möglicherweise aufgefordert, Ihre Erlaubnis zu erteilen bzw. ein Kennwort einzugeben, um Aufgaben ausführen zu können, wie das Installieren von Anwendungen, Ausführen von Dienstprogramme oder Ändern der Windows Einstellungen. Weitere Informationen hierzu finden Sie unter Hilfe und Support.

   Windows Vista – Klicken Sie auf **Jetzt defragmentieren**.

   HINWEIS: Windows verfügt über die Benutzerkontensteuerung, um die Sicherheit des Computers zu erhöhen. Sie werden möglicherweise aufgefordert, Ihre Erlaubnis zu erteilen bzw. ein Kennwort einzugeben, um Aufgaben ausführen zu können, wie das Installieren von Anwendungen, Ausführen von Dienstprogrammen oder Ändern der Windows Einstellungen. Weitere Informationen hierzu finden Sie unter Hilfe und Support.

Weitere Informationen finden Sie in der Hilfe zur Defragmentierung.

Verwenden der Datenträgerbereinigung

Bei der Datenträgerbereinigung wird die Festplatte nach nicht benötigten Dateien durchsucht. Diese können bedenkenlos gelöscht werden, um Platz auf dem Datenträger freizugeben und den Computer leistungsfähiger zu machen.

So verwenden Sie die Datenträgerbereinigung:

1. Wählen Sie **Start > Alle Programme > Zubehör > Systemprogramme > Datenträgerbereinigung**.
2. Folgen Sie den Anleitungen auf dem Bildschirm.

Verwenden von HP 3D DriveGuard (bestimmte Modelle)

HP 3D DriveGuard schützt die Festplatte, indem in den folgenden Situationen die Festplatte in die Parkposition gebracht wird und Datenanforderungen vorübergehend gestoppt werden:

- Der Computer wird fallen gelassen.
- Der Computer wird mit geschlossenem Display bei Akkubetrieb bewegt.

Kurz nachdem eine Situation dieser Art behoben wurde, versetzt HP 3D DriveGuard die Festplatte wieder in den Normalbetrieb.

HINWEIS: Da Solid-State-Laufwerke (SSDs) nicht über bewegliche Teile verfügen, ist HP 3D DriveGuard nicht erforderlich.

HINWEIS: HP 3D DriveGuard schützt Festplatten im primären Festplattenschacht und im sekundären Festplattenschacht. Festplatten, die sich in einem optionalen Dockinggerät befinden oder an einen USB-Anschluss angeschlossen sind, werden nicht von HP 3D DriveGuard geschützt.

Weitere Informationen finden Sie in der Hilfe zur HP 3D DriveGuard Software.

Ermitteln des Status von HP 3D DriveGuard

Die Laufwerksanzeige am Computer ändert die Farbe, wenn sich ein Laufwerk im primären Festplattenschacht oder ein Laufwerk im sekundären Festplattenschacht (bestimmte Modelle) in der Parkposition befindet. Verwenden Sie das Symbol rechts außen im Infobereich der Taskleiste, um festzustellen, ob gegenwärtig Laufwerke geschützt werden oder ob sich ein Laufwerk in der Parkposition befindet.

- Bei aktivierter Software wird das Festplattensymbol von einem grünen Häkchen überlagert.
- Bei deaktivierter Software wird das Festplattensymbol von einem roten X überlagert.
- Wenn sich die Laufwerke in der Parkposition befinden, wird das Festplattensymbol von einem gelben Mond überlagert.

Wenn das Symbol im Infobereich nicht aktiviert ist, führen Sie folgende Schritte aus, um es zu aktivieren:

1. Wählen Sie **Start > Systemsteuerung > Hardware und Sound > HP 3D DriveGuard**.

   HINWEIS: Klicken Sie auf **Fortsetzen**, wenn Sie von der Benutzerkontensteuerung dazu aufgefordert werden.

2. Klicken Sie unter **Symbol in der Taskleiste** auf **Einblenden**.
3. Klicken Sie auf **OK**.

Energieverwaltung bei einer „geparkten“ Festplatte

Wenn HP 3D DriveGuard das Laufwerk in die Parkposition gebracht hat, verhält sich der Computer folgendermaßen:

- Der Computer lässt sich nicht herunterfahren.
- Der Computer leitet nur in der folgenden Situation den Energiesparmodus oder Ruhezustand ein:

  HINWEIS: Wenn der Computer mit Akkuenergie betrieben wird und einen kritischen Akkuladestand erreicht, lässt HP 3D DriveGuard das Einleiten des Ruhezustands zu.

- Der Computer aktiviert nicht die Akkualarme, die auf der Registerkarte „Alarme“ in den Energieoptionen eingestellt sind.

HP empfiehlt, vor dem Transportieren des Computers entweder das System herunterzufahren oder den Energiesparmodus oder den Ruhezustand einzuleiten.

Verwenden der HP 3D DriveGuard Software

Die HP 3D DriveGuard Software ermöglicht die Durchführung folgender Aufgaben:

- Aktivieren und Deaktivieren von HP 3D DriveGuard.

  HINWEIS: Abhängig von Ihren Benutzerberechtigungen sind Sie unter Umständen nicht in der Lage, HP 3D DriveGuard zu aktivieren bzw. zu deaktivieren. Außerdem können Administratoren die Berechtigungen für Benutzer ohne Administratorrechte ändern.

- Feststellen, ob ein Laufwerk im System unterstützt wird.

So öffnen Sie die Software und ändern die Einstellungen:

1. Doppelklicken Sie auf das Symbol im Infobereich rechts außen in der Taskleiste.

   – ODER –

   Klicken Sie mit der rechten Maustaste auf das Symbol im Infobereich, und wählen Sie **Einstellungen**.

2. Klicken Sie auf die entsprechende Schaltfläche, um die Einstellungen zu ändern.
3. Klicken Sie auf **OK**.

Verwenden von optischen Laufwerken (bestimmte Modelle)

Optische Laufwerke umfassen Laufwerke der folgenden Typen:

- CD
- DVD
- Blu-ray (BD)

Ermitteln des installierten optischen Laufwerks

▲ Wählen Sie **Start > Computer**.

Alle auf dem Computer installierten Geräte werden angezeigt, auch das optische Laufwerk.

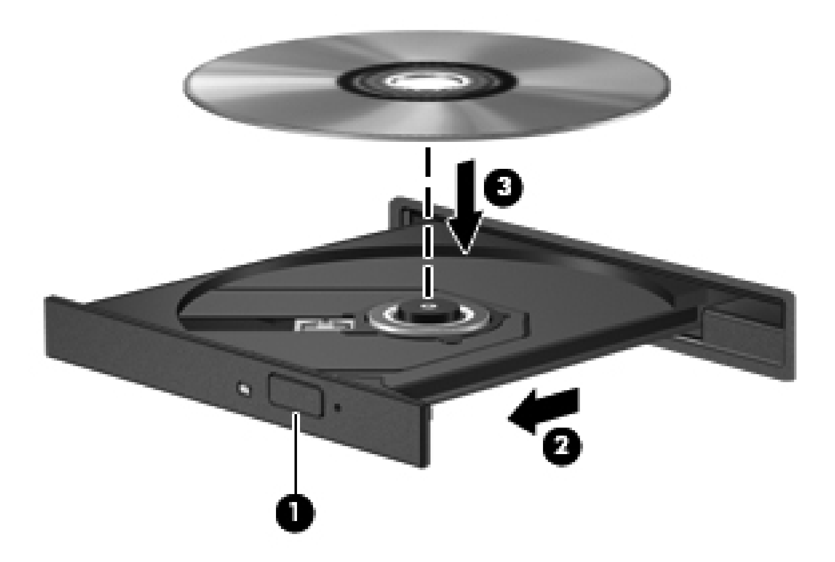
Einlegen einer optischen Disc

Medienfach

1. Schalten Sie den Computer ein.
2. Drücken Sie die Auswurftaste **(1)** an der Frontblende des Laufwerks, um das Medienfach zu entriegeln.
3. Ziehen Sie das Fach **(2)** heraus.
4. Fassen Sie die Disc am Rand und nicht an der Disc-Oberfläche an, und legen Sie sie mit der beschrifteten Seite nach oben auf die Spindel des Medienfachs.

   HINWEIS: Wenn sich das Medienfach nicht vollständig herausziehen lässt, kippen Sie die Disc leicht, um sie auf die Spindel zu legen.

5. Drücken Sie die Disc **(3)** vorsichtig bis zum Einrasten auf die Spindel im Medienfach.



6. Schließen Sie das Medienfach.

HINWEIS: Eine kurze Pause nach dem Einlegen einer Disc ist normal. Falls Sie keine Anwendung zur Medienwiedergabe ausgewählt haben, wird das Dialogfeld „Automatische Wiedergabe“ (in Windows 7) bzw. „AutoPlay“ (in Windows XP) geöffnet. Legen Sie hier fest, wie der Medieninhalt verwendet werden soll.

Einsteckschlitz

ACHTUNG: Legen Sie keine optischen **8-cm**-Discs in ein optisches Laufwerk mit Einsteckschlitz ein. Dies kann zu Beschädigungen des optischen Laufwerks führen.

1. Schalten Sie den Computer ein.
2. Fassen Sie die Disc am Rand und nicht an der Disc-Oberfläche an, und halten Sie sie mit der beschrifteten Seite nach oben.
3. Schieben Sie die Disc vorsichtig in den Einsteckschlitz des optischen Laufwerks ein.



Entfernen einer optischen Disc

Medienfach

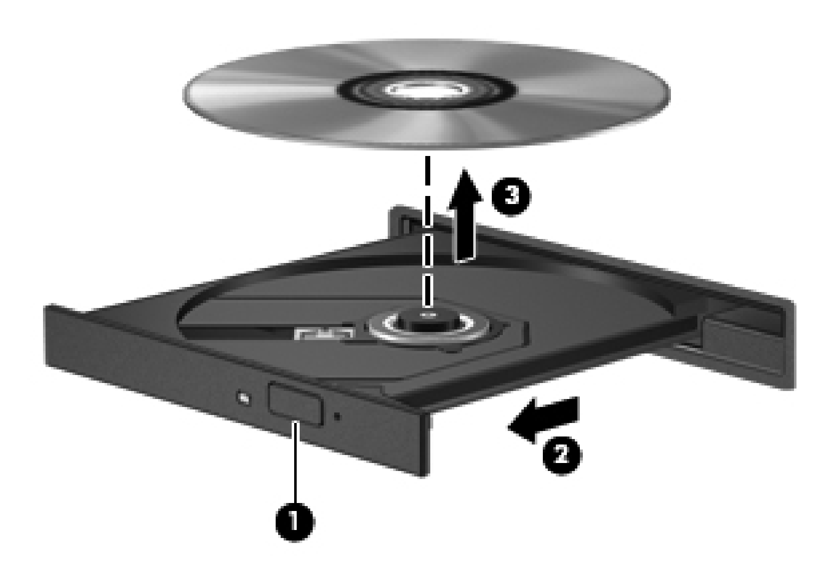
Je nachdem, ob sich das Medienfach mithilfe der Auswurftaste öffnen lässt, stehen Ihnen zwei Möglichkeiten zum Entnehmen einer Disc zur Verfügung.

Wenn sich das Medienfach normal öffnen lässt

1. Drücken Sie die Auswurftaste **(1)** an der Frontblende des Laufwerks, um das Medienfach zu entriegeln, und ziehen Sie es dann vorsichtig bis zum Anschlag heraus **(2)**.

2. Nehmen Sie die Disc **(3)** aus dem Medienfach, indem Sie die Spindel behutsam nach unten drücken, während Sie den Rand der Disc nach oben ziehen. Fassen Sie die Disc am Rand und nicht an den Oberflächen an.

   HINWEIS: Wenn sich das Medienfach nicht vollständig herausziehen lässt, kippen Sie die Disc vorsichtig beim Herausnehmen.



3. Schließen Sie das Medienfach, und bewahren Sie die Disc in einer Schutzhülle auf.

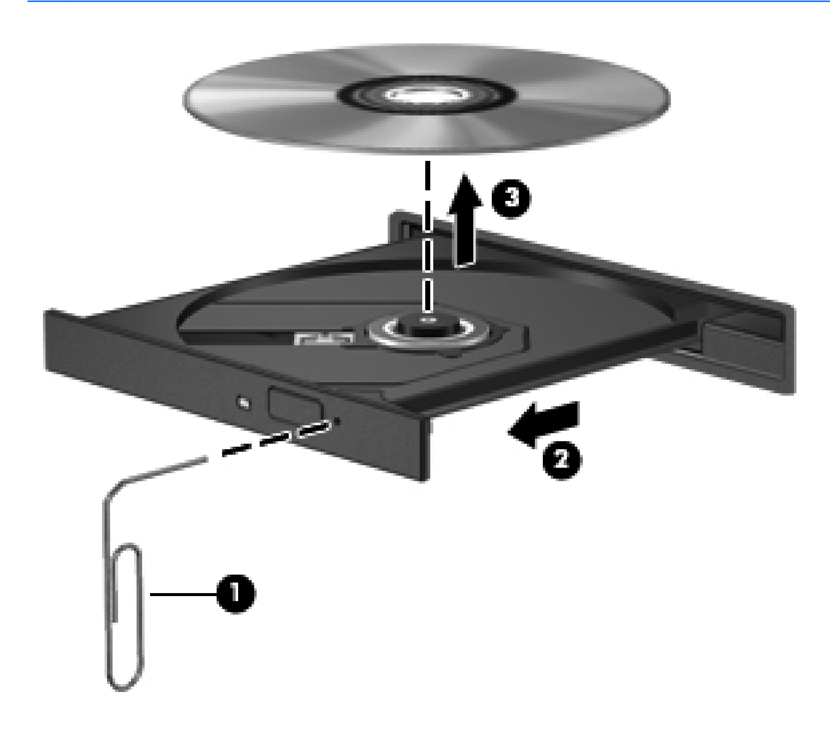
Wenn sich das Medienfach nicht normal öffnen lässt

1. Führen Sie eine aufgebogene Büroklammer **(1)** in die Freigabeöffnung an der Frontblende des Laufwerks ein.

2. Drücken Sie die Büroklammer vorsichtig hinein, bis das Medienfach entriegelt wird, und ziehen Sie es dann vollständig heraus **(2)**.

3. Nehmen Sie die Disc **(3)** aus dem Medienfach, indem Sie die Spindel behutsam nach unten drücken, während Sie den Rand der Disc nach oben ziehen. Fassen Sie die Disc am Rand und nicht an den Oberflächen an.

HINWEIS: Wenn sich das Medienfach nicht vollständig herausziehen lässt, kippen Sie die Disc vorsichtig beim Herausnehmen.



4. Schließen Sie das Medienfach, und bewahren Sie die Disc in einer Schutzhülle auf.

Einsteckschlitz

1. Drücken Sie die Auswurftaste **(1)** neben dem Laufwerk.
2. Entnehmen Sie die Disc **(2)**, indem Sie sie am Rand und nicht an den Oberflächen festhalten.



3. Bewahren Sie die Disc in einer Schutzhülle auf.

Gemeinsame Nutzung optischer Laufwerke

Auch wenn Ihr Computer nicht über ein integriertes optisches Laufwerk verfügt, können Sie auf Software und Daten zugreifen oder Anwendungen installieren, indem Sie über Ihr Netzwerk auf ein optisches Laufwerk eines anderen Computers zugreifen. Das Freigeben von Laufwerken ist eine Funktion des Windows Betriebssystems, das die Nutzung eines Laufwerks in einem Computer durch andere Computer in demselben Netzwerk ermöglicht.

HINWEIS: Um ein optisches Laufwerk gemeinsam nutzen zu können, muss ein Netzwerk eingerichtet sein. Weitere Informationen zum Einrichten eines Netzwerks finden Sie unter „Netzwerkfunktionen (bestimmte Modelle)“ auf Seite 2.

HINWEIS: Einige Discs, wie DVD-Filme und Spiele-Discs, sind möglicherweise urheberrechtlich geschützt. Diese DVDs oder CDs können nicht gemeinsam genutzt werden.

So nutzen Sie ein optisches Laufwerk gemeinsam:

1. Klicken Sie auf dem Computer, auf dem das optische Laufwerk installiert ist, auf **Start > Computer**.
2. Klicken Sie mit der rechten Maustaste auf das optische Laufwerk, das Sie freigegeben möchten, und anschließend auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte „Freigabe“ und dann auf **Erweiterte Freigabe**.
4. Markieren Sie das Kontrollkästchen **Diesen Ordner freigeben**.
5. Geben Sie einen Namen für das optische Laufwerk in das Textfeld „Freigabename“ ein.
6. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
7. Um das freigegebene optische Laufwerk auf Ihrem Computer anzuzeigen, wählen Sie **Start > Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter**.

Verwenden von RAID (bestimmte Modelle)

Die RAID (Redundant Arrays of Independent Disks)-Technologie ermöglicht es Computern, zwei oder mehr Festplatten gleichzeitig zu verwenden. Mit RAID werden mehrere Laufwerke durch bestimmte Hardware- oder Softwareeinstellungen wie ein zusammenhängendes Laufwerk behandelt. Wenn mehrere Festplatten so konfiguriert sind, dass sie auf diese Weise zusammenarbeiten, werden sie als RAID-Array bezeichnet.

Weitere Informationen zu RAID finden Sie im *RAID-Benutzerhandbuch* unter Hilfe und Support oder auf der HP Website unter http://www.hp.com/support.

7 Sicherheit

Schützen des Computers

Die Standard-Sicherheitsfunktionen des Betriebssystems Windows sowie des nicht zu Windows gehörenden Computer Setup schützen Ihre persönlichen Einstellungen und Daten vor verschiedenen Sicherheitsrisiken.

HINWEIS: Sicherheitslösungen sollen zur Abschreckung dienen. Sie können die missbräuchliche Verwendung und den Diebstahl eines Produkts jedoch nicht in jedem Fall verhindern.

HINWEIS: Bevor Sie Ihren Computer einem Servicepartner übergeben, sichern und löschen Sie alle vertraulichen Dateien und löschen Sie alle Kennworteinstellungen.

HINWEIS: Einige der in diesem Kapitel aufgelisteten Funktionen stehen möglicherweise nicht auf Ihrem Computer zur Verfügung.

HINWEIS: Ihr Computer unterstützt CompuTrace, einen Online-Sicherheitsservice zum Wiederauffinden gestohlener Computer, der in bestimmten Regionen verfügbar ist. Wenn Ihr Computer gestohlen wird, kann CompuTrace den Computer orten, wenn der unautorisierte Benutzer auf das Internet zugreift. Um CompuTrace verwenden zu können, müssen Sie die Software erwerben und den Service abonnieren. Informationen zum Bestellen der CompuTrace Software finden Sie auf der HP Website unter http://www.hpshopping.com.

Computerrisiko	Sicherheitsfunktion
Unberechtigte Verwendung des Computers	HP ProtectTools Security Manager in Verbindung mit einem Kennwort, einer Smart Card und/oder einem Fingerabdruck-Lesegerät
Unberechtigter Zugriff auf Computer Setup (f10)	BIOS-Administratorkennwort in Computer Setup*
Unberechtigter Zugriff auf den Inhalt einer Festplatte	DriveLock Kennwort in Computer Setup*
Unberechtigtes Starten von einem optischen Laufwerk, einer Diskette oder einem internen Netzwerkadapter	Boot-Optionsfunktion in Computer Setup*
Unberechtigter Zugriff auf ein Windows Benutzerkonto	HP ProtectTools Security Manager
Unberechtiger Datenzugriff	• Firewallsoftware • Windows Updates • Drive Encryption for HP ProtectTools
Unberechtigter Zugriff auf die Einstellungen von Computer Setup und andere Informationen zur Identifizierung des Systems	BIOS-Administratorkennwort in Computer Setup*

Computerrisiko	Sicherheitsfunktion
Unberechtigtes Entfernen des Computers	Öffnung für die Diebstahlsicherung (in Verbindung mit einem optionalen Sicherheitskabel)
*Computer Setup ist ein vorinstalliertes, auf ROM basierendes Utility, das selbst dann verwendet werden kann, wenn das Betriebssystem nicht reagiert oder sich nicht laden lässt. Sie können entweder mit einem Zeigegerät (TouchPad, Pointing Stick oder USB-Maus) oder der Tastatur navigieren und in Computer Setup eine Auswahl treffen.	

Verwenden von Kennwörtern

Ein Kennwort ist eine Gruppe von Zeichen, die Sie zum Schutz der Computerdaten auswählen. Je nachdem, wie Sie den Zugriff auf Ihre Daten steuern möchten, können Sie verschiedene Kennworttypen einrichten. Kennwörter können unter Windows oder im nicht in Windows integrierten, vorinstallierten Computer Setup eingerichtet werden.

- Setup- und DriveLock Kennwörter werden in Computer Setup festgelegt und vom System-BIOS verwaltet.
- Das Embedded Security-Kennwort, bei dem es sich um ein Kennwort von HP ProtectTools Security Manager handelt, kann in Computer Setup aktiviert werden, so dass neben den normalen HP ProtectTools Funktionen noch ein zusätzlicher BIOS-Kennwortschutz besteht. Das Embedded Security-Kennwort wird zusammen mit dem optionalen integrierten Security-Chip verwendet.
- Windows Kennwörter werden nur im Windows Betriebssystem eingerichtet.
- Wenn Sie das BIOS-Administratorkennwort, das in Computer Setup festgelegt wurde, vergessen, können Sie das Utility mit HP SpareKey aufrufen.
- Wenn Sie sowohl das Benutzerkennwort als auch das DriveLock Master-Kennwort, die beide in Computer Setup eingerichtet wurden, vergessen haben, ist die kennwortgeschützte Festplatte dauerhaft gesperrt und kann nicht mehr verwendet werden.

Sie können für eine Funktion von Computer Setup und für eine Windows Sicherheitsfunktion dasselbe Kennwort verwenden. Außerdem ist es möglich, ein und dasselbe Kennwort für mehrere Computer Setup-Funktionen zu vergeben.

Tipps zum Erstellen und Speichern von Kennwörtern:

- Erfüllen Sie beim Erstellen von Kennwörtern die vom Programm festgelegten Anforderungen.
- Notieren Sie Ihre Kennwörter, und bewahren Sie diese Informationen an einem sicheren Ort und auf keinen Fall zusammen mit dem Computer auf.
- Speichern Sie die Kennwörter nicht in einer Datei auf dem Computer.

In der folgenden Tabelle sind die in der Regel verwendeten Windows und BIOS-Administratorkennwörter aufgeführt und beschrieben.

Einrichten von Kennwörtern in Windows

Kennwort	Funktion
Administratorkennwort*	Schützt den Zugriff auf ein Konto auf Windows Administratorebene. **HINWEIS:** Dieses Kennwort kann nicht verwendet werden, um die Daten von Computer Setup aufzurufen.
Benutzerkennwort*	Schützt den Zugriff auf ein Windows Benutzerkonto.
*Informationen zum Einrichten eines Windows Administratorkennworts oder Windows Benutzerkennworts finden Sie unter **Start > Hilfe und Support**.	

Einrichten von Kennwörtern in Computer Setup

Kennwort	Funktion
BIOS-Administratorkennwort*	Schützt vor dem Zugriff auf Computer Setup.
DriveLock-Master-Kennwort*	Schützt vor dem Zugriff auf die interne Festplatte, die durch DriveLock geschützt ist. Wird auch zum Aufheben der DriveLock Sperre verwendet. Dieses Kennwort wird während des Aktivierungsvorgangs unter „DriveLock Kennwort“ eingerichtet.
DriveLock-Benutzerkennwort*	Schützt vor dem Zugriff auf die interne, durch DriveLock geschützte Festplatte und wird während des Aktivierungsvorgangs unter „DriveLock Kennwort“ eingerichtet.
TPM Embedded Security-Kennwort	Schützt bei Aktivierung als BIOS-Administratorkennwort vor dem Zugriff auf die Daten des Computers, wenn der Computer eingeschaltet oder neu gestartet wird oder wenn der Ruhezustand beendet wird. Für dieses Kennwort wird der optionale integrierte Sicherheits-Chip benötigt, damit die zugehörige Sicherheitsfunktion unterstützt werden kann.
*Weitere Informationen zu den einzelnen Kennwörtern finden Sie in den folgenden Abschnitten.	

Verwalten eines BIOS-Administratorkennworts

So können Sie dieses Kennwort einrichten, ändern oder löschen:

Einrichten eines neuen BIOS-Administratorkennworts

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie esc, wenn die Meldung „Press the ESC key for Startup Menu“ (ESC drücken, um Startmenü zu öffnen) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> Setup BIOS Administrator Password** (BIOS-Administratorkennwort einrichten), und drücken Sie dann die Eingabetaste.
4. Geben Sie bei entsprechender Aufforderung ein Kennwort ein.
5. Geben Sie das neue Kennwort bei entsprechender Aufforderung erneut ein, um es zu bestätigen.
6. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie anschließend die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Ändern eines BIOS-Administratorkennworts

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie esc, wenn die Meldung „Press the ESC key for Startup Menu“ (ESC drücken, um Startmenü zu öffnen) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> Change Password** (Kennwort ändern), und drücken Sie dann die Eingabetaste.
4. Geben Sie bei entsprechender Aufforderung das aktuelle Kennwort ein.
5. Geben Sie bei entsprechender Aufforderung das neue Kennwort noch einmal ein, um es zu bestätigen.
6. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie anschließend die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Löschen eines BIOS-Administratorkennworts

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie esc, wenn die Meldung „Press the ESC key for Startup Menu“ (ESC drücken, um Startmenü zu öffnen) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> Change Password** (Kennwort ändern), und drücken Sie dann die Eingabetaste.
4. Geben Sie bei entsprechender Aufforderung das aktuelle Kennwort ein.
5. Lassen Sie das entsprechende Eingabefeld leer, wenn Sie zur Eingabe des neuen Kennworts aufgefordert werden. Drücken Sie die Eingabetaste.
6. Lesen Sie den Warnhinweis. Wählen Sie zur Fortsetzung des Vorgangs **YES** (Ja).
7. Lassen Sie das entsprechende Eingabefeld leer, wenn Sie noch einmal zur Eingabe des neuen Kennworts aufgefordert werden. Drücken Sie die Eingabetaste.
8. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie anschließend die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Eingeben eines BIOS-Administratorkennworts

Geben Sie im Dialogfeld **BIOS-Administratorkennwort** das Kennwort ein. Verwenden Sie dieselben Tasten wie beim Einrichten des Kennworts, und drücken Sie die Eingabetaste. Wurde das BIOS-Administratorkennwort drei Mal falsch eingegeben, muss der Computer neu gestartet werden, damit weitere Versuche möglich sind.

Verwalten eines DriveLock Kennworts in Computer Setup

ACHTUNG: Um zu verhindern, dass die mit DriveLock geschützte Festplatte auf Dauer unbrauchbar wird, notieren Sie das DriveLock Benutzerkennwort und das DriveLock Master-Kennwort, und bewahren Sie sie an einem sicheren Ort separat vom Computer auf. Wenn Sie beide DriveLock Kennwörter vergessen, ist die Festplatte dauerhaft gesperrt und kann nicht mehr verwendet werden.

DriveLock verhindert den unberechtigten Zugriff auf die Daten einer Festplatte. Die Schutzfunktion von DriveLock steht nur für die internen Festplatten des Computers zur Verfügung. Nachdem DriveLock für ein Laufwerk eingerichtet wurde, ist der Zugriff auf dieses Laufwerk erst nach Eingabe eines Kennworts möglich. Auf ein Laufwerk oder einen erweiterten Portreplikator kann nur dann über DriveLock Kennwörter zugegriffen werden, wenn das Laufwerk bzw. der Portreplikator in den Computer eingebaut ist.

Um DriveLock für interne Festplatten verwenden zu können, muss in Computer Setup sowohl ein Benutzerkennwort als auch ein Master-Kennwort eingerichtet werden. Beachten Sie die folgenden Hinweise zur Verwendung von DriveLock:

- Nachdem die DriveLock Sperre für eine Festplatte eingerichtet wurde, ist der Zugriff auf diese Festplatte erst nach Eingabe des Benutzer- oder Master-Kennworts möglich.
- Eigentümer des Benutzerkennworts sollte daher der Benutzer sein, der täglich mit der geschützten Festplatte arbeitet. Der Inhaber des Master-Kennworts kann ein Systemadministrator oder der übliche Benutzer sein.
- Benutzerkennwort und Master-Kennwort können identisch sein.
- Sie können ein Benutzer- oder Master-Kennwort nur löschen, indem Sie den DriveLock Schutz des Laufwerks aufheben. Der DriveLock Schutz für eine Festplatte kann nur durch Eingabe des Master-Kennworts deaktiviert werden.

Einrichten eines DriveLock Kennworts

So richten Sie ein DriveLock Kennwort in Computer Setup ein:

1. Schalten Sie den Computer ein, drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> DriveLock Passwords** (DriveLock Kennwörter), und drücken Sie dann die Eingabetaste.
4. Klicken Sie mit einem Zeigegerät auf die zu schützende Festplatte.

   – ODER –

   Wählen Sie die zu schützende Festplatte mit den Pfeiltasten aus, und drücken Sie die Eingabetaste.

5. Lesen Sie die Warnmeldung. Wählen Sie **YES** (Ja), um fortzufahren.

6. Geben Sie bei entsprechender Aufforderung ein Master-Kennwort ein, und drücken Sie die Eingabetaste.

7. Geben Sie bei entsprechender Aufforderung erneut das Master-Kennwort ein, um es zu bestätigen, und drücken Sie die Eingabetaste.

8. Geben Sie bei entsprechender Aufforderung ein Benutzerkennwort ein, und drücken Sie die Eingabetaste.

9. Geben Sie bei entsprechender Aufforderung das Benutzerkennwort erneut ein, um es zu bestätigen, und drücken Sie die Eingabetaste.

10. Zum Bestätigen des DriveLock Schutzes für das ausgewählte Laufwerk geben Sie `DriveLock` in das Bestätigungsfeld ein, und drücken Sie die Eingabetaste.

    HINWEIS: Bei der DriveLock Bestätigung wird zwischen Groß- und Kleinschreibung unterschieden.

11. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

    – ODER –

    Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Eingeben eines DriveLock Kennworts

Stellen Sie sicher, dass die Festplatte im Computer und nicht in einem optionalen Dockingprodukt oder einer externen MultiBay eingesetzt ist.

Wenn Sie zur Eingabe eines DriveLock Kennworts aufgefordert werden, geben Sie das Benutzer- oder das Master-Kennwort mit den Tasten desselben Typs ein, die bei seiner Festlegung verwendet wurden, und drücken Sie die Eingabetaste.

Wurde das Kennwort zwei Mal falsch eingegeben, muss der Computer zunächst heruntergefahren werden, damit weitere Versuche möglich sind.

Ändern eines DriveLock Kennworts

So ändern Sie ein DriveLock Kennwort in Computer Setup:

1. Schalten Sie den Computer ein, drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu" (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> DriveLock Password** (DriveLock Kennwort), und drücken Sie dann die Eingabetaste.
4. Wählen Sie mit einem Zeigegerät eine interne Festplatte.

   – ODER –

   Wählen Sie mit den Pfeiltasten eine interne Festplatte, und drücken Sie die Eingabetaste.
5. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten das zu ändernde Kennwort.
6. Geben Sie bei entsprechender Aufforderung Ihr aktuelles Kennwort ein, und drücken Sie die Eingabetaste.
7. Geben Sie bei entsprechender Aufforderung ein neues Kennwort ein, und drücken Sie die Eingabetaste.
8. Geben Sie bei entsprechender Aufforderung das neue Kennwort erneut ein, um es zu bestätigen, und drücken Sie die Eingabetaste.
9. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Aufheben des DriveLock Schutzes

So entfernen Sie den DriveLock Schutz in Computer Setup:

1. Schalten Sie den Computer ein, drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> DriveLock Password** (DriveLock Kennwort), und drücken Sie dann die Eingabetaste.
4. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten eine interne Festplatte, und drücken Sie die Eingabetaste.
5. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten die Option **Disable protection** (Schutz deaktivieren).
6. Geben Sie Ihr Master-Kennwort ein, und drücken Sie die Eingabetaste.
7. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie anschließend die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Verwenden des automatischen DriveLock von Computer Setup

In einer Mehrbenutzerumgebung können Sie ein Kennwort für den automatischen DriveLock einrichten. Wenn das Kennwort für den automatischen DriveLock aktiviert ist, werden ein nach dem Zufallsprinzip generiertes Benutzerkennwort und ein DriveLock Master-Kennwort für Sie erstellt. Wenn ein Benutzer die Kennwortanmeldung erfolgreich abschließt, wird dieses per Zufall generierte Benutzerkennwort und das DriveLock Master-Kennwort zum Entsperren des Laufwerks verwendet.

HINWEIS: Sie müssen über ein BIOS-Administratorkennwort verfügen, bevor Sie auf die Funktionen des automatischen DriveLock zugreifen können.

Eingeben eines Kennworts für den automatischen DriveLock

So aktivieren Sie ein Kennwort für den automatischen DriveLock in Computer Setup:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> Automatic DriveLock** (Automatischer DriveLock), und drücken Sie die Eingabetaste.
4. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten eine interne Festplatte, und drücken Sie die Eingabetaste.

5. Lesen Sie die Warnmeldung. Wählen Sie **YES** (Ja), um fortzufahren.

6. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie anschließend die Eingabetaste.

Aufheben des automatischen DriveLock Schutzes

So entfernen Sie den DriveLock Schutz in Computer Setup:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.

2. Drücken Sie f10, um Computer Setup zu starten.

3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **Security** (Sicherheit) **> Automatic DriveLock** (Automatischer DriveLock), und drücken Sie die Eingabetaste.

4. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten eine interne Festplatte, und drücken Sie die Eingabetaste.

5. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten die Option **Disable protection** (Schutz deaktivieren).

6. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie anschließend die Eingabetaste.

Verwenden von Antivirensoftware

Wenn Sie den Computer für E-Mail-Kommunikation, Netzwerk- oder Internetzugang verwenden, setzen Sie ihn möglicherweise Computerviren aus. Computerviren können das Betriebssystem, Anwendungen oder Dienstprogramme funktionsunfähig machen oder ihre Funktion beeinträchtigen.

Antivirensoftware kann die meisten Viren erkennen, zerstören und in den meisten Fällen den durch sie verursachten Schaden reparieren. Um dauerhaften Schutz vor neu entdeckten Viren zu gewährleisten, muss die Antivirensoftware regelmäßig aktualisiert werden.

Möglicherweise ist ein Antivirenprogramm auf Ihrem Computer vorinstalliert, das Sie für einen bestimmten Zeitraum testen können. Es wird dringend empfohlen, ein Upgrade für die Testversion bzw. ein anderes Antivirenprogramm Ihrer Wahl zu erwerben, damit Ihr Computer vollständig geschützt ist.

Um weitere Informationen über Computerviren zu erhalten, geben Sie `Viren` in das Suchfeld unter Hilfe und Support ein.

Verwenden von Firewallsoftware

Firewalls sollen unberechtigte Zugriffe auf ein System oder Netzwerk verhindern. Eine Firewall kann eine Software sein, die Sie auf dem Computer und/oder Netzwerk installieren, es kann sich jedoch auch um eine Lösung handeln, die sowohl Hardware als auch Software umfasst.

Es gibt zwei Arten von Firewalls, die für Sie von Bedeutung sein könnten:

- Host-basierte Firewalls – Software, die nur den Computer schützt, auf dem sie installiert ist.
- Netzwerk-basierte Firewalls – Wird zwischen dem DSL- oder Kabelmodem und dem Heimnetzwerk installiert und schützt alle Computer im Netzwerk.

Wenn eine Firewall auf einem System installiert ist, werden alle Daten, die an dieses bzw. von diesem System gesendet werden, überwacht und mit einer Reihe von benutzerdefinierten Sicherheitskriterien verglichen. Alle Daten, die diese Kriterien nicht erfüllen, werden blockiert.

Auf Ihrem Computer oder Ihren Netzwerkgeräten wurde möglicherweise schon eine Firewall installiert. Andernfalls sind Firewallsoftwarelösungen erhältlich.

HINWEIS: Unter bestimmten Umständen kann eine Firewall den Zugriff auf Internetspiele verhindern, die gemeinsame Nutzung von Druckern und Dateien in einem Netzwerk beeinträchtigen oder autorisierte E-Mail-Anhänge blockieren. Um solche Probleme vorübergehend zu beheben, deaktivieren Sie die Firewall, führen Sie die gewünschte Aufgabe durch, und aktivieren Sie die Firewall dann wieder. Sie können das Problem dauerhaft beheben, indem Sie die Firewall neu konfigurieren.

Installieren wichtiger Sicherheitsupdates

⚠ **ACHTUNG:** Microsoft sendet Benachrichtigungen, wenn wichtige Updates verfügbar sind. Zum Schutz Ihres Computers vor Sicherheitslücken und Viren sollten Sie alle kritischen Updates von Microsoft installieren, sobald Sie eine entsprechende Benachrichtigung erhalten.

Nach Auslieferung Ihres Computers wurden möglicherweise zusätzliche Updates für das Betriebssystem und andere auf dem Computer enthaltene Software zur Verfügung gestellt. So sorgen Sie dafür, dass alle verfügbaren Updates auf Ihrem Computer installiert sind:

- Führen Sie Windows Update gleich aus, wenn Sie Ihren Computer eingerichtet haben.
- Führen Sie Windows Update danach einmal im Monat aus.
- Sie können Updates für Windows und andere Microsoft Programme sofort nach deren Veröffentlichung von der Microsoft Website und über den Link zu den Updates unter Hilfe und Support beziehen.

Verwenden von HP ProtectTools Security Manager (bestimmte Modelle)

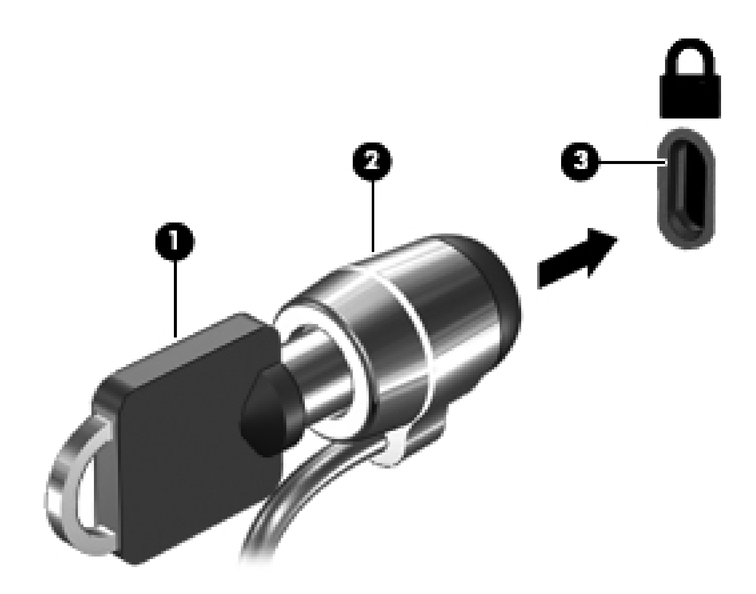
Auf bestimmten Computermodellen ist HP ProtectTools Security Manager vorinstalliert. Diese Software erreichen Sie über die Windows Systemsteuerung. Sie enthält Sicherheitsfunktionen, die vor unberechtigtem Zugriff auf den Computer, Netzwerke und kritische Daten schützen. Weitere Informationen finden Sie in der Online-Hilfe von HP ProtectTools.

Installieren einer optionalen Diebstahlsicherung

HINWEIS: Eine Diebstahlsicherung soll der Abschreckung dienen, kann eine missbräuchliche Verwendung oder einen Diebstahl des Computers jedoch nicht in jedem Fall verhindern.

HINWEIS: Möglicherweise unterscheidet sich die Öffnung für die Diebstahlsicherung am Computer optisch leicht von der Abbildung in diesem Abschnitt. Informationen zur Position der Öffnung für die Diebstahlsicherung am Computer finden Sie im Handbuch *Einführung*.

1. Schlingen Sie die Diebstahlsicherung um einen feststehenden Gegenstand.
2. Stecken Sie den Schlüssel **(1)** in das Kabelschloss der Diebstahlsicherung **(2)**.
3. Stecken Sie das Kabelschloss in die Öffnung für die Diebstahlsicherung am Computer **(3)**, und verschließen Sie das Kabelschloss anschließend mit dem Schlüssel.



Verwenden des Fingerabdruck-Lesegeräts (bestimmte Modelle)

Integrierte Fingerabdruck-Lesegeräte sind bei bestimmten Modellen verfügbar. Um das Fingerabdruck-Lesegerät nutzen zu können, müssen Sie auf dem Computer ein Benutzerkonto mit Kennwort einrichten. Über dieses Konto können Sie sich anschließend durch Bewegen eines festgelegten Fingers über dem Lesegerät am Computer anmelden. Sie können das Fingerabdruck-Lesegerät auch verwenden, um Kennwortfelder auf Websites und in anderen Programmen, für die eine Anmeldung erforderlich ist, auszufüllen. Eine Anleitung finden Sie in der Hilfe der Fingerabdruck-Software.

Nachdem Sie Ihre Fingerabdruck-Identität erstellt haben, können Sie einen Dienst für Einmaliges Anmelden (Single Sign On, SSO) einrichten, der es Ihnen ermöglicht, den Fingerabduck-Scanner zum Erstellen von Anmeldeinformationen für alle Anwendungen zu verwenden, die einen Benutzernamen und ein Kennwort erfordern.

Position des Fingerabdruck-Lesegeräts

Das Fingerabdruck-Lesegerät ist ein kleiner, metallener Sensor, der sich in einem der folgenden Bereiche am Computer befindet:

- An der Unterseite des TouchPad
- Auf der rechten Seite der Tastatur
- Oben rechts am Display
- Links am Display

Je nach Computermodell ist das Fingerabdruck-Lesegerät horizontal oder vertikal ausgerichtet. Bei beiden Ausrichtungen ist es erforderlich, dass Sie Ihren Finger senkrecht zum Metallsensor bewegen. Informationen zur Position des Fingerabdruck-Lesegeräts am Computer finden Sie im Handbuch *Einführung*.

8 Wartung

Reinigung und Pflege Ihres Computers

Reinigungsmittel

Verwenden Sie folgende Reinigungsmittel, um Ihr Notebook bzw. Ihren Tablet PC schonend zu reinigen und zu desinfizieren:

- Dimethylbenzylammoniumchlorid mit einer Konzentration von max. 0,3 Prozent (z. B. desinfizierende Einwegtücher. Diese Tücher werden von vielen verschiedenen Marken angeboten.)
- Alkoholfreien Glasreiniger
- Wasser mit milder Seifenlösung
- Trockenes Mikrofaser-Reinigungstuch oder Ledertuch (antistatisches Tuch ohne Öl)
- Antistatische Stofftücher

⚠ **ACHTUNG:** Folgende Reinigungsmittel sollten nicht verwendet werden:

Starke Lösungsmittel, beispielsweise Alkohol, Aceton, Ammoniumchlorid, Methylenchlorid und Kohlenwasserstoffe, können die Oberfläche des Notebooks oder Tablet PC dauerhaft beschädigen.

Faserstoffe wie Papiertücher können Kratzer auf dem Notebook bzw. Tablet PC hinterlassen. Im Laufe der Zeit können sich Schmutzpartikel und Reinigungsmittel in den Kratzern ansammeln.

Reinigungsverfahren

Gehen Sie anhand der in diesem Kapitel beschriebenen Verfahren vor, um Ihr Notebook oder Ihren Tablet PC schonend zu reinigen.

⚠ **VORSICHT!** Um einen Stromschlag oder einen Schaden an den Komponenten zu verhindern, reinigen Sie Ihr Notebook bzw. den Tablet PC nicht, während dieses bzw. dieser eingeschaltet ist.

Schalten Sie das Notebook bzw. den Tablet PC aus.

Trennen Sie den Computer von der externen Stromversorgung.

Trennen Sie die Verbindung zu allen externen Geräten mit eigener Stromversorgung.

⚠ **ACHTUNG:** Sprühen Sie keine Reinigungsmittel oder Flüssigkeiten direkt auf Notebook- oder Tablet PC-Oberflächen. Flüssigkeiten, die auf die Oberfläche geraten, können interne Komponenten dauerhaft beschädigen.

Reinigen des Displays

Wischen Sie das Display vorsichtig mit einem weichen, fusselfreien Tuch ab, das zuvor mit einem *alkoholfreien* Glasreiniger befeuchtet wurde. Stellen Sie sicher, dass das Display trocken ist, bevor Sie es schließen.

Reinigen der Seiten und des Deckels

Um die Seiten und den Deckel zu reinigen und zu desinfizieren, verwenden Sie ein weiches Mikrofasertuch oder Ledertuch mit einem der vorstehend aufgeführten Reinigungsmittel, oder verwenden Sie ein geeignetes desinfizierendes Einwegtuch.

HINWEIS: Reinigen Sie den Deckel des Notebooks in kreisenden Bewegungen, um Schmutz zu entfernen.

Reinigen des TouchPad und der Tastatur

ACHTUNG: Achten Sie beim Reinigen des TouchPad und der Tastatur darauf, dass keine Flüssigkeit zwischen die Tasten gerät. Dadurch könnten interne Komponenten permanent beschädigt werden.

- Um TouchPad und Tastatur zu reinigen und zu desinfizieren, verwenden Sie ein weiches Mikrofasertuch oder Ledertuch mit einem der vorstehend aufgeführten Reinigungsmittel, oder verwenden Sie ein geeignetes desinfizierendes Einwegtuch.
- Verwenden Sie eine Druckluftflasche mit Röhrchenaufsatz, um zu verhindern, dass sich die Tasten verklemmen und um Staub, Fussel und andere Fremdkörper, die sich auf bzw. in der Tastatur ansammeln können, zu entfernen.

  VORSICHT! Verwenden Sie zum Reinigen der Tastatur keinen Staubsaugeraufsatz, um Stromschläge und Beschädigungen der internen Komponenten zu vermeiden. Durch einen Staubsauger kann Haushaltsschmutz auf die Computeroberfläche gelangen.

Reinigen eines Tablet PC-Stifts und Stifthalters

Befeuchten Sie ein weiches Mikrofasertuch oder Ledertuch mit einem der vorstehend aufgeführten Reinigungsmittel, oder verwenden Sie ein geeignetes desinfizierendes Einwegtuch:

- Um den Stift zu reinigen, reiben Sie den Stift von oben nach unten ab, um Schmutz zu entfernen.
- Reinigen Sie den Stifthalter mit kreisenden Bewegungen um die Öffnung des Stifthalters herum.

ACHTUNG: Achten Sie darauf, dass keine Flüssigkeit bzw. andere Materialien als der Tablet PC-Stift in den Stifthalter gelangen. Der Stifthalter ist von einigen internen Komponenten des Tablet PCs nicht abgeschottet.

Aktualisieren von Programmen und Treibern

HP empfiehlt, Ihre Programme und Treiber regelmäßig mit der neuesten Version zu aktualisieren. Rufen Sie die Website http://www.hp.com/support auf, um die neuesten Versionen herunterzuladen. Sie können sich auch registrieren, um automatisch benachrichtigt zu werden, sobald ein Update verfügbar ist.

Verwenden von SoftPaq Download Manager

Mit dem Tool HP SoftPaq Download Manager (SDM) können Sie schnell auf Informationen über SoftPaqs für HP Business-Computer zugreifen, ohne die SoftPaq-Nummer eingeben zu müssen. Mit diesem Tool können Sie bequem nach SoftPaqs suchen und diese anschließend herunterladen und entpacken.

SoftPaq Download Manager liest eine veröffentlichte Datenbankdatei mit Informationen über SoftPaqs und Computermodelle und lädt die Datei von der HP FTP-Site herunter. Mit SoftPaq Download Manager können Sie ein oder mehrere Computermodelle angeben, um festzustellen, welche SoftPaqs zum Download verfügbar sind.

SoftPaq Download Manager durchsucht die HP FTP-Site nach Updates der Datenbank und Software-Updates. Wenn Updates verfügbar sind, werden diese heruntergeladen und automatisch installiert.

SoftPaq Download Manager ist auf der HP Website verfügbar. Um SoftPaqs herunterzuladen, müssen Sie zunächst das Programm SoftPaq Download Manager herunterladen und installieren. Öffnen Sie die HP Website unter http://www.hp.com/go/sdm, und folgen Sie den Anleitungen zum Herunterladen und Installieren von SoftPaq Download Manager.

So laden Sie SoftPaqs herunter:

1. Wählen Sie **Start > Alle Programme > HP Software Setup > HP SoftPaq Download Manager**.
2. Wenn SoftPaq Download Manager zum ersten Mal geöffnet wird, werden Sie in einem Fenster gefragt, ob nur Software für den Computer, den Sie gerade verwenden, oder für alle unterstützten Modelle angezeigt werden soll. Wählen Sie **Software für alle unterstützten Modelle anzeigen**. Wenn Sie HP SoftPaq Download Manager bereits verwendet haben, fahren Sie mit Schritt 3 fort.
   a. Wählen Sie im Fenster **Konfigurationsoptionen** Ihr Betriebssystem und die entsprechende Sprache aus. Durch diese Filter können Sie die Anzahl der Optionen im Teilfenster **Produktkatalog** einschränken. Wenn beispielsweise nur Windows 7 Professional als Betriebssystem ausgewählt wird, wird im Produktkatalog nur das Betriebssystem Windows 7 Professional angezeigt.
   b. Um andere Betriebssysteme hinzuzufügen, ändern Sie die Filtereinstellungen im Fenster **Konfigurationsoptionen**. Weitere Informationen finden Sie in der Hilfe zur HP SoftPaq Download Manager Software.
3. Klicken Sie im linken Teilfenster auf das Pluszeichen (+), um die Modellliste zu erweitern, und wählen Sie dann das Modell bzw. die Modelle der Produkte aus, die Sie aktualisieren möchten.
4. Klicken Sie auf **Nach verfügbaren SoftPaqs suchen**, um eine Liste der verfügbaren SoftPaqs für den ausgewählten Computer herunterzuladen.
5. Wählen Sie von den verfügbaren SoftPaqs die gewünschten SoftPaqs aus, und klicken Sie auf **Nur herunterladen**, wenn Sie viele SoftPaqs herunterladen möchten. Die Dauer des Download-Vorgangs hängt von der Anzahl der ausgewählten SoftPaqs und der Geschwindigkeit der Internetverbindung ab.

   Wenn Sie nur ein oder zwei SoftPaqs herunterladen möchten und über eine Hochgeschwindigkeits-Internetanbindung verfügen, klicken Sie auf **Herunterladen und Entpacken**.
6. Führen Sie in SoftPaq Download Manager einen Rechtsklick auf **SoftPaq installieren** aus, um die ausgewählten SoftPaqs auf dem Computer zu installieren.

9 Computer Setup (BIOS) und System Diagnostics (Systemdiagnose)

Verwenden von Computer Setup

Computer Setup oder Basic Input/Output System (BIOS) steuert die Kommunikation zwischen allen Eingabe- und Ausgabegeräten im System (z. B. Laufwerke, Anzeige, Tastatur, Maus und Drucker). Computer Setup umfasst Einstellungen für die installierten Gerätetypen, die Startreihenfolge des Computers sowie die Größe des Systemspeichers und des erweiterten Speichers.

HINWEIS: Gehen Sie äußerst vorsichtig vor, wenn Sie Änderungen in Computer Setup vornehmen. Fehler können dazu führen, dass der Computer nicht mehr ordnungsgemäß funktioniert.

Starten von Computer Setup

HINWEIS: Eine über den USB-Anschluss angeschlossene externe Tastatur oder Maus kann in Computer Setup nur verwendet werden, wenn die betriebssystemunabhängige USB-Unterstützung aktiviert ist.

So starten Sie Computer Setup:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.

Navigieren und Auswählen in Computer Setup

So navigieren Sie in Computer Setup und wählen Optionen:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.

   - Zum Wählen eines Menüs oder eines Menüelements verwenden Sie die Tabulatortaste und die Pfeiltasten der Tastatur und drücken die Eingabetaste. Sie können auch mit einem Zeigegerät auf das Element klicken.
   - Um einen Bildlauf nach oben oder unten durchzuführen, klicken Sie rechts oben im Bildschirm auf den Aufwärts- bzw. Abwärtspfeil, oder verwenden Sie die Nach-oben- bzw. die Nach-unten-Taste.
   - Um Dialogfelder zu schließen und zum Hauptbildschirm von Computer Setup zurückzukehren, drücken Sie die esc-Taste, und folgen Sie den Anleitungen auf dem Bildschirm.

   HINWEIS: Sie können entweder mit einem Zeigegerät (TouchPad, Pointing Stick oder USB-Maus) oder der Tastatur navigieren und in Computer Setup eine Auswahl treffen.

2. Drücken Sie f10, um Computer Setup zu starten.

Verlassen Sie die Computer Setup-Menüs mit einem der folgenden Verfahren:

- So beenden Sie Computer Setup, ohne die Änderungen aus der aktuellen Sitzung zu speichern:

  Klicken Sie in der unteren linken Bildschirmecke auf das Symbol **Exit** (Beenden), und folgen Sie den Anleitungen auf dem Bildschirm.

  – ODER –

  Wählen Sie mithilfe der Tabulatortaste oder der Pfeiltasten **File** (Datei) **> Ignore Changes and Exit** (Änderungen ignorieren und beenden), und drücken Sie dann die Eingabetaste.

- So speichern Sie Ihre Änderungen und beenden Computer Setup:

  Klicken Sie in der unteren linken Bildschirmecke auf das Symbol **Save** (Speichern), und folgen Sie den Anleitungen auf dem Bildschirm.

  – ODER –

  Wählen Sie mithilfe der Tabulatortaste oder der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Wiederherstellen der Standardeinstellungen in Computer Setup

HINWEIS: Beim Wiederherstellen der Standardeinstellungen wird der Festplattenmodus nicht geändert.

So setzen Sie in Computer Setup die Einstellungen wieder auf den Lieferzustand zurück:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie die esc-Taste, wenn die Meldung „Press the ESC key for Startup Menu“ (Zum Aufrufen des Startup-Menüs ESC-Taste drücken) unten im Bildschirm angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **File** (Datei) **> Restore Defaults** (Standardeinstellungen wiederherstellen).
4. Folgen Sie den Anleitungen auf dem Bildschirm.
5. Um Ihre Änderungen zu speichern und zu beenden, klicken Sie auf **Save** (Speichern) unten links im Bildschirm, und folgen Sie dann den angezeigten Anleitungen.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

HINWEIS: Die Einstellungen für Kennwörter und Sicherheit werden beim Wiederherstellen der Standardeinstellungen nicht verändert.

Aktualisieren des BIOS

Auf der HP Website sind möglicherweise aktualisierte Versionen der Software erhältlich, die mit Ihrem Computer geliefert wurde.

Die meisten Software und BIOS-Updates, die von der HP Website heruntergeladen werden können, liegen als komprimierte Dateien namens *SoftPaqs* vor.

Einige Softwarepakete, die heruntergeladen werden können, enthalten eine Infodatei (README.TXT), die Hinweise zur Installation und zur Fehlerbeseitigung der Datei enthält.

Ermitteln der BIOS-Version

Um festzustellen, ob die verfügbaren BIOS-Updates aktueller als die auf Ihrem Computer installierte BIOS-Version sind, müssen Sie zunächst die Version Ihres momentan vorhandenen System-BIOS ermitteln.

BIOS-Versionsinformationen (auch *ROM-Datum* und *System BIOS* genannt) können durch Drücken von fn+esc (wenn Sie sich bereits in Windows befinden) oder mithilfe von Computer Setup angezeigt werden.

1. Starten Sie Computer Setup.
2. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **File** (Datei) **> System Information** (Systeminformationen).
3. Klicken Sie links unten im Bildschirm auf **Exit** (Beenden), um Ihre Änderungen zu verwerfen und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Tabulatortaste oder der Pfeiltasten **File** (Datei) **>Ignore Changes and Exit** (Änderungen ignorieren und beenden). Drücken Sie dann die Eingabetaste.

Herunterladen eines BIOS-Update

ACHTUNG: Um das Risiko von Schäden am Computer oder einer fehlerhaften Installation zu verringern, sollten Sie ein Update des System-BIOS nur herunterladen und installieren, wenn der Computer über das Netzteil an eine zuverlässige externe Stromquelle angeschlossen ist. Ein BIOS-Update sollte nicht heruntergeladen oder installiert werden, solange der Computer mit Akkus betrieben wird, mit einem optionalen Dockinggerät verbunden oder an eine optionale Stromquelle angeschlossen ist. Beim Herunterladen und Installieren muss Folgendes beachtet werden:

Unterbrechen Sie nicht die Stromzufuhr zum Gerät, indem Sie das Netzkabel aus der Steckdose ziehen.

Schalten Sie den Computer nicht aus, und leiten Sie nicht den Energiesparmodus oder Ruhezustand ein.

Es dürfen keine Geräte eingesetzt oder entfernt oder Kabel angeschlossen bzw. abgezogen werden.

1. Wählen Sie **Start > Hilfe und Support > Systempflege**.
2. Folgen Sie den Anleitungen auf dem Bildschirm, um Ihren Computer zu ermitteln und auf das BIOS-Update zuzugreifen, das Sie herunterladen möchten.
3. Gehen Sie im Download-Bereich wie folgt vor:
   - **a.** Suchen Sie nach dem BIOS-Update, das aktueller ist als die derzeitige BIOS-Version auf Ihrem Computer. Notieren Sie sich Datum, Name bzw. andere Kennzeichnungen. Möglicherweise benötigen Sie diese Informationen später, um das Update nach dem Herunterladen auf Ihrer Festplatte zu identifizieren.
   - **b.** Folgen Sie den Anleitungen auf dem Bildschirm, um das ausgewählte Update auf die Festplatte herunterzuladen.

     Notieren Sie sich den Pfad auf Ihrer Festplatte, auf den das BIOS-Update heruntergeladen wurde. Sie müssen bei der Installation des Updates auf diesen Pfad zugreifen.

   HINWEIS: Wenn Sie Ihren Computer in ein Netzwerk einbinden, sprechen Sie vor der Installation von Software-Updates, insbesondere von System-BIOS-Updates, mit Ihrem Netzwerkadministrator.

Es gibt verschiedene Installationsverfahren für BIOS-Updates. Befolgen Sie die Anleitungen, die nach dem Herunterladen auf dem Bildschirm angezeigt werden. Wenn keine Anleitungen angezeigt werden, gehen Sie folgendermaßen vor:

1. Öffnen Sie Windows Explorer, indem Sie **Start > Computer** wählen.
2. Doppelklicken Sie auf Ihre Festplatte. Dies ist im Allgemeinen „Lokaler Datenträger (C:)".
3. Öffnen Sie auf dem zuvor notierten Pfad auf der Festplatte den Ordner, in dem sich das Update befindet.
4. Doppelklicken Sie auf die Datei mit der Dateierweiterung .exe (zum Beispiel *Dateiname*.exe).

   Der Installationsvorgang wird gestartet.
5. Führen Sie die Installation anhand der Anleitungen auf dem Bildschirm durch.

HINWEIS: Wenn eine Meldung über die erfolgreiche Installation angezeigt wird, können Sie die heruntergeladene Datei von Ihrer Festplatte löschen.

Verwenden von System Diagnostics (Systemdiagnose)

Mit System Diagnostics (Systemdiagnose) können Sie Diagnosetests ausführen, um festzustellen, ob die Computerhardware ordnungsgemäß funktioniert. Die folgenden Diagnosetests stehen in System Diagnostics (Systemdiagnose) zur Verfügung:

- Start-up test (Systemstarttest) – Mithilfe dieses Tests werden die Hauptkomponenten des Computers überprüft, die für den Start des Computers erforderlich sind.
- Run-in test (Lasttest) – Bei diesem Test wird der Systemstarttest wiederholt. Dabei wird eine Überprüfung auf zeitweise auftretende Probleme durchgeführt, die der Systemstarttest nicht erkennt.
- Hard disk test (Festplattentest) – Bei diesem Test werden der physische Zustand der Festplatte sowie sämtliche Daten in allen Sektoren der Festplatte überprüft. Wird beim Test ein beschädigter Sektor ermittelt, wird versucht, die Daten in einen unbeschädigten Sektor zu verschieben.
- Memory test (Speichertest) – Bei diesem Test wird der physische Zustand der Speichermodule überprüft. Wird ein Fehler berichtet, müssen Sie die Speichermodule sofort austauschen.
- Battery test (Akkutest) – Bei diesem Test wird der Zustand des Akkus überprüft. Wenn der Akku den Test nicht besteht, wenden Sie sich an den HP Kundensupport, um das Problem zu berichten und einen Ersatzakku zu erwerben.

Im Fenster „System Diagnostics“ (Systemdiagnose) können Sie außerdem Systeminformationen und Fehlerprotokolle anzeigen.

So starten Sie „System Diagnostics“ (Systemdiagnose):

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie die esc-Taste, wenn links unten im Bildschirm die Meldung „Press the ESC key for Startup Menu“ (ESC drücken, um Startmenü zu öffnen) angezeigt wird. Wenn das Startmenü angezeigt wird, drücken Sie f2.
2. Klicken Sie auf den Diagnosetest, den Sie ausführen möchten, und folgen Sie dann den Anleitungen auf dem Bildschirm.

HINWEIS: Wenn Sie den Diagnosetest beenden müssen, während er ausgeführt wird, drücken Sie esc.

10 MultiBoot

Bootgerätereihenfolge

Beim Computerstart versucht das System, von den aktivierten Bootgeräten zu booten. Das standardmäßig aktivierte MultiBoot Utility bestimmt die Reihenfolge, in der das System die Bootgeräte auswählt. Bootgeräte können optische Laufwerke, Diskettenlaufwerke, eine Netzwerkkarte (NIC), Festplatten und USB-Geräte sein. Bootgeräte enthalten bootfähige Medien oder Dateien, die der Computer zum Starten und für einen ordnungsgemäßen Betrieb benötigt.

HINWEIS: Einige Bootgeräte müssen erst in Computer Setup aktiviert werden, bevor sie in die Bootreihenfolge aufgenommen werden können.

Werksseitig ist der Computer so eingestellt, dass er das Bootgerät auswählt, indem er die aktivierten Bootgeräte und Laufwerkspositionen in der folgenden Reihenfolge durchsucht:

HINWEIS: Möglicherweise werden einige der Bootgeräte und Laufwerkspositionen nicht von Ihrem Computer unterstützt.

- Notebook-Erweiterungsschacht
- Optisches Laufwerk
- Notebook-Festplatte
- USB-Diskettenlaufwerk
- USB-CD-ROM
- USB-Festplatte
- Notebook Ethernet
- Secure Digital (SD)-Speicherkarte
- Dockingstation-Erweiterungsschacht
- Externes SATA-Laufwerk

Sie können die Reihenfolge ändern, in der der Computer nach einem Bootgerät sucht, indem Sie die Startreihenfolge in Computer Setup ändern. Sie können auch esc drücken, während die Meldung „Press the ESC key for Startup Menu“ (ESC drücken, um das Startmenü zu öffnen) unten im Bildschirm angezeigt wird, und anschließend f9 drücken. Durch Drücken von f9 wird ein Menü angezeigt, in dem die aktuellen Bootgeräte aufgelistet werden und Sie ein Bootgerät auswählen können. Sie können den Computer mit MultiBoot Express auch so einrichten, dass Sie beim Einschalten oder Neustarten zur Eingabe eines Boot-Orts aufgefordert werden.

Aktivieren von Bootgeräten in Computer Setup

Der Computer kann nur dann von einem USB-Gerät oder einer Netzwerkkarte starten, wenn das Gerät zuvor in Computer Setup aktiviert wurde.

So starten Sie Computer Setup und aktivieren ein USB-Gerät oder eine Netzwerkkarte als Bootgerät:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie esc, während die Meldung „Press the ESC key for Startup Menu“ (ESC-Taste drücken, um Startmenü zu öffnen) am unteren Bildschirmrand angezeigt wird.

2. Drücken Sie f10, um Computer Setup zu starten.

3. Zur Aktivierung von bootfähigen Medien in USB-Laufwerken oder in Laufwerken, die in ein optionales Dockinggerät eingelegt wurden, wählen Sie mit einem Zeigegerät oder mit den Pfeiltasten **System Configuration** (Systemkonfiguration) **> Device Configurations** (Gerätekonfigurationen). Bestätigen Sie, dass die **Betriebssystemunabhängige USB-Unterstützung** ausgewählt ist.

   HINWEIS: Die Option für den USB-Anschluss muss aktiviert sein, damit die betriebssystemunabhängige USB-Unterstützung verwendet werden kann. Die Option ist werksseitig aktiviert. Wenn der Anschluss deaktiviert wird, aktivieren Sie ihn erneut, indem Sie **System Configuration** (Systemkonfiguration) **> Port Options** (Anschlussoptionen) und anschließend **USB Port** (USB-Anschluss) auswählen.

   – ODER –

   Um ein NIC-Gerät zu aktivieren, wählen Sie **System Configuration** (Systemkonfiguration) **> Boot Options** (Startoptionen) und anschließend **PXE Internal NIC boot** (PXE-Bootvorgang über interne NIC).

4. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

HINWEIS: Zum Verbinden einer Netzwerkkarte mit einem PXE- oder RPL-Server (PXE = Preboot eXecution Environment; RPL = Remote Program Load) ohne MultiBoot drücken Sie die Taste esc, wenn die Meldung „Press the ESC key for Startup Menu“ (ESC-Taste drücken, um Startmenü zu öffnen) am unteren Bildschirmrand erscheint. Drücken Sie anschließend schnell f12.

Erwägungen bei der Auswahl der Bootreihenfolge

Bevor Sie die Bootreihenfolge ändern, sollten Sie Folgendes bedenken:

- Beim Neustart nach einer Änderung der Bootreihenfolge versucht der Computer, anhand der neuen Bootreihenfolge zu starten.
- Wenn mehr als ein Bootgerätetyp vorhanden ist, versucht der Computer vom ersten Gerät jedes Bootgerätetyps (außer optische Geräte) zu booten. Wenn der Computer beispielsweise an ein optionales Dockinggerät angeschlossen ist (bestimmte Modelle), das eine Festplatte enthält, wird diese Festplatte in der Bootreihenfolge als USB-Festplatte angezeigt. Wenn das System versucht, von dieser USB-Festplatte zu booten, und der Versuch fehlschlägt, versucht das System nicht, von der Festplatte im Festplattenschacht zu booten. Stattdessen versucht es, vom nächsten Gerätetyp in der Bootreihenfolge zu booten. Sind jedoch zwei optische Laufwerke vorhanden, versucht das System, wenn das erste optische Gerät nicht bootet (weil es keine Medien enthält oder weil das Medium keine Boot-Disc ist), über das zweite optische Laufwerk zu booten.
- Änderungen der Bootreihenfolge wirken sich auch auf die Zuordnung der Laufwerksbuchstaben aus. Wenn Sie beispielsweise mit einer als Laufwerk C formatierten CD von einem CD-ROM-Laufwerk starten, wird dieses CD-ROM-Laufwerk zu Laufwerk C, und die Festplatte im Festplattenschacht wird zu Laufwerk D.
- Der Computer kann nur dann von einem NIC-Gerät starten, wenn das Gerät zuvor im Menü „Built-in device options“ (Optionen für integrierte Geräte) von Computer Setup aktiviert wurde und wenn das Starten von diesem Gerät im Menü „Boot options“ (Startoptionen) von Computer Setup aktiviert ist. Da der Netzwerkkarte kein Laufwerksbuchstabe zugeordnet ist, bleiben beim Starten von einer Netzwerkkarte die Bezeichnungen der logischen Laufwerke unverändert.
- Die Laufwerke in einem optionalen Dockinggerät (nur bestimmte Modelle) werden in der Bootreihenfolge wie externe USB-Geräte behandelt.

Wählen der MultiBoot Einstellungen

Sie können MultiBoot auf verschiedene Arten einsetzen:

- Zum Festlegen einer neuen Bootreihenfolge beim Computerstart, indem Sie in Computer Setup die Bootreihenfolge ändern.
- Zur dynamischen Auswahl des Bootgeräts, indem Sie die Taste esc drücken, während am unteren Bildschirmrand die Meldung „Press the ESC key for Startup Menu“ (ESC-Taste drücken, um Startmenü zu öffnen) angezeigt wird. Drücken Sie anschließend f9, um das Menü für Bootgeräte-Optionen zu öffnen.
- Zum Einstellen variabler Bootreihenfolgen mithilfe von MultiBoot Express. Bei Verwendung dieser Funktion werden Sie bei jedem Start oder Neustart des Computers zur Angabe des Bootgeräts aufgefordert.

Festlegen einer neuen Bootreihenfolge in Computer Setup

So starten Sie Computer Setup und legen eine neue Bootreihenfolge fest, die der Computer bei jedem Start oder Neustart verwendet:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie esc, wenn die Meldung „Press the ESC key for Startup Menu“ (ESC-Taste drücken, um Startmenü zu öffnen) am unteren Bildschirmrand angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder mit den Pfeiltasten die Liste **Legacy Boot Order** (Betriebssystemunabhängige Startreihenfolge) aus. Drücken Sie dann die Eingabetaste.
4. Klicken Sie mit einem Zeigegerät auf den Pfeil nach oben, oder drücken Sie die Taste + auf der Tastatur, um das Gerät in der Startreihenfolge nach oben zu verschieben.

   – ODER –

   Klicken Sie mit einem Zeigegerät auf den Pfeil nach unten, oder drücken Sie die Taste - auf der Tastatur, um das Gerät in der Startreihenfolge nach unten zu verschieben.
5. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Dynamisches Auswählen eines Bootgeräts mit F9

So wählen Sie dynamisch ein Bootgerät für die aktuelle Startsequenz aus:

1. Öffnen Sie das Menü „Select Boot Device“ (Bootgerät auswählen), indem Sie den Computer einschalten oder neu starten und die Taste esc drücken, während die Meldung „Press the ESC key for Startup Menu“ (ESC-Taste drücken, um Startmenü zu öffnen) am unteren Bildschirmrand angezeigt wird.
2. Drücken Sie f9.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten ein Bootgerät aus, und drücken Sie die Eingabetaste.

Die Änderungen werden sofort wirksam.

Festlegen einer MultiBoot Express-Eingabeaufforderung

So starten Sie Computer Setup und legen fest, dass bei jedem Start oder Neustart des Computers das MultiBoot-Bootmenü angezeigt wird:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Drücken Sie esc, wenn die Meldung „Press the ESC key for Startup Menu“ (ESC-Taste drücken, um Startmenü zu öffnen) am unteren Bildschirmrand angezeigt wird.
2. Drücken Sie f10, um Computer Setup zu starten.
3. Wählen Sie mit einem Zeigegerät oder den Pfeiltasten **System Configuration** (Systemkonfiguration) **> Boot Options** (Boot-Optionen), und drücken Sie anschließend die Eingabetaste.
4. Geben Sie im Feld **Multiboot Express Popup Delay (Sec)** (Verzögerung für MultiBoot-Popup (Sek.)) an, wie viele Sekunden das Bootmenü angezeigt werden soll, bevor die aktuelle MultiBoot Einstellung berücksichtigt wird. (Wenn 0 ausgewählt wird, wird das Express Boot-Menü nicht angezeigt.)
5. Klicken Sie links unten im Bildschirm auf das Symbol **Save** (Speichern), um Ihre Änderungen zu speichern und Computer Setup zu beenden. Folgen Sie anschließend den Anleitungen auf dem Bildschirm.

   – ODER –

   Wählen Sie mithilfe der Pfeiltasten **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden), und drücken Sie dann die Eingabetaste.

Die Änderungen werden beim Neustart des Computers wirksam.

Festlegen der MultiBoot Express-Einstellungen

Wenn das Express-Bootmenü beim Start angezeigt wird, haben Sie folgende Möglichkeiten:

- Soll ein bestimmtes Bootgerät im Express-Bootmenü angegeben werden, wählen Sie die gewünschte Einstellung im vorgegebenen Zeitrahmen, und drücken Sie anschließend die Eingabetaste.
- Soll der Computer nicht die aktuelle MultiBoot-Einstellung verwenden, drücken Sie vor Ablauf der vorgegebenen Zeit eine beliebige Taste. Der Computer startet erst, wenn Sie ein Bootgerät ausgewählt und die Eingabetaste gedrückt haben.
- Soll der Computer mit den aktuellen MultiBoot-Einstellungen starten, lassen Sie die vorgegebene Zeit einfach verstreichen.

11 Verwaltung

Verwenden von Client Management Solutions

Die Client Management Solutions-Software bietet auf Standards basierende Lösungen für die Verwaltung von Client (Anwender)-Desktops, -Workstations, -Notebooks und -Tablet PCs in einer Netzwerkumgebung.

Zu den wichtigsten Funktionen und Merkmalen des Clientmanagements gehören:

- Deployment von anfänglichen Software-Images
- Remoteinstallation von Systemsoftware
- Softwaremanagement und -Updates
- ROM-Updates
- Verfolgung und Sicherheit von Computerbeständen (die im Computer installierte Hardware und Software)
- Fehlerbenachrichtigung und Wiederherstellung für bestimmte Systemsoftware und Hardwarekomponenten

HINWEIS: Inwieweit bestimmte in diesem Abschnitt beschriebene Funktionen jeweils unterstützt werden, hängt vom Computermodell bzw. der Version der auf dem Computer installierten Managementsoftware ab.

Konfigurieren und Deployment eines Software-Image

Der Computer wird mit einem vorinstallierten Systemsoftware-Image ausgeliefert. Das anfängliche Software-Image wird während des ersten Setup des Computers konfiguriert. Nach einem kurzen Entbündelungs-Vorgang ist der Computer einsatzbereit.

Das Deployment (die Verteilung) eines benutzerdefinierten Software-Image kann wie folgt geschehen:

- Installieren zusätzlicher Softwareanwendungen nach dem Entbündeln des vorinstallierten Software-Image
- Verwenden von Software-Deployment-Tools, beispielsweise Altiris Deployment Solutions, um die vorinstallierte Software durch ein benutzerdefiniertes Software-Image zu ersetzen
- Verwenden eines Verfahrens zum Klonen von Festplatten, um den Inhalt einer Festplatte auf eine andere zu kopieren

Welche Deployment-Methode Sie nutzen, hängt von der technologischen Umgebung und den Prozessen Ihrer Organisation ab.

HINWEIS: Computer Setup und andere Systemfunktionen bieten Ihnen weitere Unterstützung bei Konfigurationsmanagement und Fehlerbeseitigung, Energieverwaltung und Wiederherstellung der Systemsoftware.

Verwalten und Aktualisieren von Software

HP bietet verschiedene Tools für das Verwalten und Aktualisieren von Software auf Clientcomputern:

- HP Client Manager for Altiris (bestimmte Modelle)

  HINWEIS: Besuchen Sie die HP Website unter http://www.hp.com, um von dort HP Client Manager for Altiris herunterzuladen oder weitere Informationen darüber zu erhalten.

- HP CCM (Client Configuration Manager) (bestimmte Modelle)
- HP SSM (System Software Manager)

HP Client Manager for Altiris (bestimmte Modelle)

HP Client Manager for Altiris kombiniert die Intelligent Manageability-Technologie mit der Altiris Software und stellt einzigartige Hardware-Verwaltungsfunktionen für HP Geräte bereit:

- Detaillierte Ansichten des Hardwarebestands für das Bestandsmanagement
- Überwachung und Diagnose des Systems
- Über das Web zugängliche Berichte über aufgabenkritische Details, wie Warnmeldungen wegen Überhitzung oder Speicherproblemen
- Remote-Update von Systemsoftware, wie Gerätetreibern und dem System-BIOS

HINWEIS: Zusätzliche Funktionen stehen zur Verfügung, wenn HP Client Manager for Altiris zusammen mit der optionalen Altiris Solutions Software (separat zu erwerben) eingesetzt wird.

Bei Verwendung von HP Client Manager for Altiris (auf einem Client-Computer installiert) in Verbindung mit Altiris Solutions (auf einem Administrator-Computer installiert) bietet HP Client Manager for Altiris erweiterte Verwaltungsfunktionen und eine zentrale Hardware-Verwaltung der Client-Geräte für folgende Bereiche des IT-Lebenszyklus:

- Inventar- und Bestandsmanagement
  - Einhaltung von Softwarelizenzen
  - Verfolgung von Computern und Berichterstellung
  - Informationen über Leasingverträge für Computer und Verfolgung von Anlagegegenständen
- Deployment und Migration von Systemsoftware
  - Windows Migration
  - System-Deployment
  - Migration von persönlichen Benutzereinstellungen

- Helpdesk und Problembehebung
  - Verwalten von Helpdesk-Tickets
  - Remote-Fehlerbeseitigung
  - Remote-Problembehebung
  - Clientfehlerkorrektur
- Software- und Betriebsmanagement
  - Kontinuierliches Clientmanagement
  - Deployment von HP Systemsoftware
  - Selbstheilung von Anwendungen (Fähigkeit zur Erkennung und Reparatur bestimmter Anwendungsprobleme)

Die Altiris Solutions Software bietet benutzerfreundliche Funktionen für die Softwareverteilung. HP Client Manager for Altiris ermöglicht die Kommunikation mit Altiris Solutions, um das Deployment neuer Hardwarekomponenten oder die Migration von persönlichen Benutzereinstellungen auf ein neues Betriebssystem mithilfe von Assistenten durchzuführen. HP Client Manager for Altiris kann von der HP Website heruntergeladen werden.

Bei Einsatz von Altiris Solutions zusammen mit HP System Software Manager oder dem HP Client Manager for Altiris können Administratoren auch das System-BIOS und die Gerätetreibersoftware über eine zentrale Konsole aktualisieren.

HP CCM (Client Configuration Manager) (bestimmte Modelle)

HP CCM automatisiert die Verwaltung von Software, wie z. B. von Betriebssystemen, Programmen, Software-Updates, sowie Content- und Konfigurationseinstellungen. Dadurch wird sichergestellt, dass jeder Computer mit der ordnungsgemäßen Konfiguration ausgeführt wird. Mithilfe dieser Lösungen zur automatisierten Verwaltung können Sie die Software während des gesamten Lebenszyklus des Computers verwalten.

Mit CCM können Sie die folgenden Aufgaben ausführen:

- Erfassen des Hardware- und Softwarebestands auf verschiedenen Plattformen
- Vorbereiten eines Softwarepakets und Durchführen einer Auswirkungsanalyse vor der Verteilung
- Festlegen von einzelnen Computern, Arbeitsgruppen oder gesamten Computerbeständen für das Deployment und die Wartung von Software und Inhalten gemäß den Sicherheitsrichtlinien
- Bereitstellen und Verwalten von Betriebssystemen, Anwendungen und Inhalten auf Computern dezentral von jeder Stelle im Netzwerk
- Integration von CCM in Help Desks und andere Systemmanagement-Tools für übergangslose Zusammenarbeit
- Nutzen einer gemeinsamen Infrastruktur zum Verwalten von Software und Inhalten auf Standardcomputern in jedem Netzwerk für alle Benutzer im Unternehmen
- Skalieren und Anpassen an die Anforderungen des Unternehmens

HP SSM (System Software Manager)

HP SSM ermöglicht per Remote-Zugriff das Aktualisieren von Software auf Systemebene auf mehreren Systemen gleichzeitig. Bei der Ausführung auf einem Client-Computer erkennt SSM Hardware- und Software-Versionen und aktualisiert die vorgesehene Software aus einem zentralen Repository, dem so genannten Dateispeicher. Treiberversionen, die von SSM unterstützt werden, sind auf der Treiber-Downloadseite von HP und auf der *Support Software* CD mit einem klar erkennbaren Symbol versehen. Besuchen Sie die HP Website unter http://www.hp.com/go/ssm (nur Englisch), um von dort das Dienstprogramm SSM herunterzuladen oder weitere Informationen zu SSM zu erhalten.

Verwenden der Intel Active-Management-Technologie (bestimmte Modelle)

Intel® Active Management Technology (iAMT) ermöglicht das Ermitteln, Reparieren und Schützen von Computerbeständen im Netzwerk. Mit iAMT können Computer unabhängig davon verwaltet werden, ob diese ein- oder ausgeschaltet sind. Die iAMT Lösung ist auf Intel Centrino® Computern mit vPro Mobiltechnologie verfügbar.

Zu den Merkmalen von iAMT zählen folgende:

- Hardwarebestandsinformationen
- Ereignisbenachrichtigung
- Energieverwaltung
- Ferndiagnose und -reparatur
- Hardwarebasierte Isolierung und Wiederherstellung – Zugriff auf Computernetzwerk einschränken oder verhindern, wenn Aktivitäten auf einen Virus schließen lassen

Aktivieren der iAMT Lösung

So konfigurieren Sie die iAMT Einstellungen:

HINWEIS: Die strg+p-Aufforderung wird nur angezeigt, wenn die Option „AMT Setup Prompt“ (Aufforderung für AMT-Setup) in Computer Setup aktiviert ist.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
2. Bevor Windows geladen wird, drücken Sie strg+p.

   HINWEIS: Wenn Sie strg+p nicht rechtzeitig drücken, müssen Sie die Schritte 1 und 2 wiederholen, um auf das MEBx Setup-Utility zugreifen zu können.

3. Geben Sie das Kennwort für die Management Engine (ME) ein. Das werksseitig festgelegte Kennwort lautet *admin*.

   Das MEBx Setup-Utility wird geöffnet. Navigieren Sie mithilfe der Pfeiltasten.

4. Konfigurieren Sie Intel ME, iAMT, oder ändern Sie das Intel ME-Kennwort.
5. Wenn Sie Ihre Wahl getroffen haben, wählen Sie **Exit** (Beenden), um das MEBx Setup-Utility zu schließen.

Verwenden der Menüs im MEBx Setup-Utility

HINWEIS: Weitere Informationen zu iAMT erhalten Sie auf der Website von Intel unter http://www.intel.com. Geben Sie dort den Suchbegriff iAMT ein.

Intel ME Configuration

Option	Funktion
Intel ME State Control	Deaktivieren/Aktivieren der Management Engine
Intel ME Firmware Local Update	Deaktivieren/Aktivieren der lokalen Verwaltung von Firmware-Updates
LAN Controller	Deaktivieren/Aktivieren des integrierten Netzwerkcontrollers
Intel ME Features Control	AMT oder keine Funktion aktivieren/deaktivieren
Intel ME Power Control	Konfigurieren der Energierichtlinien der Management Engine

iAMT Configuration

Option	Funktion
Host Name	Zuordnen eines Hostnamens zum Computer
TCP/IP	Deaktivieren/Aktivieren der Netzwerkschnittstelle oder DHCP (ordnet eine IP-Adresse zu, wenn DHCP deaktiviert wurde) oder Ändern des Domänennamens.
Provision Model	Zuordnen eines iAMT-Modells je nach Groß- oder Kleinunternehmen
Setup and Configuration	Einstellen der Optionen zur Steuerung der Remote-Konfiguration von AMT.

Option	Funktion
Un-Provision	Zurücksetzen der AMT-Konfiguration auf Standardwerte
SOL/IDE-R	Aktivieren/Deaktivieren der Remote-Bootsteuerung von IDE-Diskette oder CD-ROM unter Zuweisung von Benutzernamen und Benutzerkennwort
Password Policy	Festlegen der Anforderungen für das Netzwerkkennwort und MEBx-Kennwort.
Secure Firmware Update	Aktivieren/Deaktivieren von Remote-Firmware-Updates
Set PRTC	Einstellen der Echtzeituhr
Idle Timeout	Festlegen eines Timeout-Werts

Change Intel ME Password

Option	Funktion
Change ME Password	Ändern des Kennworts **HINWEIS:** Das Standardkennwort lautet **admin**.

A Reisen mit dem Computer

Tipps für Reise und Transport:

- Bereiten Sie den Computer auf einen Transport oder eine Reise vor:
  - Sichern Sie Ihre Daten.
  - Entfernen Sie alle Discs und externen Speicherkarten (z. B. digitale Karten).

    ⚠ **ACHTUNG:** Um eine Beschädigung des Computers oder eines Laufwerks sowie das Risiko eines Datenverlusts möglichst gering zu halten, nehmen Sie den Datenträger aus dem Laufwerk, bevor Sie das Laufwerk aus dem Festplattenschacht entfernen, es versenden, lagern oder auf Reisen mitnehmen.

  - Schalten Sie alle externen Geräte aus, und trennen Sie sie vom Computer.
  - Schalten Sie den Computer aus.
- Nehmen Sie eine Sicherungskopie Ihrer Daten mit. Bewahren Sie die gesicherten Daten getrennt von Ihrem Computer auf.
- Nehmen Sie den Computer auf Flugreisen im Handgepäck mit; geben Sie ihn nicht mit dem restlichen Gepäck auf.

  ⚠ **ACHTUNG:** Setzen Sie Laufwerke keinen Magnetfeldern aus. Sicherheitseinrichtungen mit Magnetfeldern sind z. B. Sicherheitsschleusen und Handsucher in Flughäfen. Förderbänder und ähnliche Sicherheitseinrichtungen in Flughäfen, mit denen Handgepäck kontrolliert wird, arbeiten mit Röntgenstrahlen statt mit Magnetismus und stellen daher keine Gefahr für die Laufwerke dar.

- Die Verwendung von Computern während eines Fluges liegt im Ermessen der Fluggesellschaft. Wenn Sie den Computer während des Fluges verwenden möchten, erkundigen Sie sich zuvor bei der Fluggesellschaft, ob dies zulässig ist.
- Nehmen Sie den Akku aus dem Computer, und bewahren Sie ihn separat auf, wenn der Computer länger als zwei Wochen nicht benutzt wird und an keine externe Stromquelle angeschlossen ist.
- Wenn Sie den Computer oder ein Laufwerk per Post versenden möchten, verwenden Sie eine angemessene Schutzverpackung, und kennzeichnen Sie die Sendung als „Zerbrechlich".
- Wenn im Computer ein Wireless-Gerät oder ein HP UMTS-Modul installiert ist, wie zum Beispiel ein 802.11b/g-Gerät, ein GSM (Global System for Mobile Communications)- oder GPRS (General Packet Radio Service)-Gerät, ist die Verwendung dieser Geräte in einigen Umgebungen möglicherweise eingeschränkt. Solche Einschränkungen können an Bord von Flugzeugen, in Krankenhäusern, in der Nähe explosiver Stoffe und an anderen gefährlichen

Orten gelten. Wenn Sie nicht sicher sind, welche Richtlinien für die Verwendung eines bestimmten Geräts gelten, bitten Sie vor dem Einschalten des Geräts um die Genehmigung.

- Beachten Sie bei Auslandsreisen Folgendes:
  - Informieren Sie sich über die für Computer geltenden Zollbestimmungen der Länder und Regionen, die Sie bereisen.
  - Überprüfen Sie die Voraussetzungen hinsichtlich Netzkabel und Adapter für alle Gebiete, in denen Sie den Computer verwenden möchten. Spannung, Frequenz und Stecker unterscheiden sich in den verschiedenen Ländern/Regionen.

VORSICHT! Verwenden Sie für den Anschluss des Computers an das örtliche Stromnetz keine Spannungskonverter, die für Elektrokleingeräte angeboten werden. Es kann sonst zu Feuer, elektrischen Schlägen oder Beschädigungen kommen.

B Ressourcen für die Fehlerbeseitigung

- Rufen Sie unter Hilfe und Support weitere Informationen über den Computer sowie Website-Links auf. Wählen Sie **Start > Hilfe und Support**.

HINWEIS: Für einige Prüf- und Reparatur-Tools benötigen Sie eine Internetverbindung. HP stellt außerdem zusätzliche Tools zur Verfügung, die keine Internetverbindung erfordern.

- Wenden Sie sich an den HP Kundenservice unter http://www.hp.com/go/contactHP.

HINWEIS: Um den internationalen Support aufzurufen, klicken Sie auf **Contact HP worldwide** (Kontaktieren Sie HP in anderen Ländern/Regionen) links auf der Seite, oder navigieren Sie zu http://welcome.hp.com/country/us/en/wwcontact_us.html.

Wählen Sie eine der folgenden Support-Arten:

  - Online-Chat mit einem HP Techniker

    HINWEIS: Wenn die Chat-Option für eine bestimmte Sprache nicht verfügbar ist, ist sie in englischer Sprache verfügbar.

  - E-Mail an den HP Kundenservice
  - Nach Telefonnummern des internationalen HP Kundenservices suchen
  - Nach einem HP Service Center suchen

C Elektrostatische Entladung

Elekrostatische Entladung ist die Entladung statischer Elektrizität, wenn zwei Objekte miteinander in Kontakt kommen (z. B. der Schlag, den Sie erhalten, wenn Sie über einen Teppich laufen und eine metallene Türklinke berühren).

Eine Entladung statischer Elektrizität über Finger oder andere elektrostatische Leiter kann zu Beschädigungen von elektronischen Komponenten führen. Beachten Sie folgende Vorsichtsmaßnahmen, um Computer- oder Laufwerkschäden und den Verlust von Daten zu vermeiden:

- Wenn Sie beim Entfernen von Komponenten oder in der Installationsanleitung aufgefordert werden, den Computer auszustecken, stellen Sie sicher, dass Sie ordnungsgemäß geerdet sind, und stecken Sie den Computer aus, bevor Sie die Abdeckung entfernen.
- Entnehmen Sie Komponenten erst aus den elektrostatikgeschützten Behältnissen, wenn Sie bereit sind, diese zu installieren.
- Vermeiden Sie das Berühren von Kontakten, leitenden Komponenten und Schaltkreisen. Vermeiden Sie möglichst den Kontakt mit elektronischen Komponenten.
- Verwenden Sie unmagnetische Werkzeuge.
- Bevor Sie Arbeiten an Komponenten vornehmen, müssen Sie zunächst die statische Elektrizität entladen, indem Sie eine nicht lackierte Metalloberfläche der Komponente berühren.
- Wenn Sie eine Komponente entfernen, bewahren Sie sie in einem elektrostatikgeschützten Behältnis auf.

Wenn Sie weitere Informationen zur statischen Elektrizität oder Hilfe beim Entfernen oder Installieren von Komponenten benötigen, wenden Sie sich an den HP Kundensupport.

Index

RAID

Benutzerhandbuch

Erste Ausgabe: Mai 2011

Teilenummer des Dokuments: 651196-041

Produkthinweis

Dieses Benutzerhandbuch beschreibt die Funktionen, die auf den meisten Modellen verfügbar sind. Einige der Funktionen sind möglicherweise nicht auf Ihrem Computer verfügbar.

Inhaltsverzeichnis

1 Einführung

Bis vor kurzem hatten die meisten Computerbenutzer nur recht wenige Möglichkeiten, sich im Falle eines Festplattenausfalls vor Datenverlust zu schützen. Dazu gehörten das manuelle Kopieren von Dateien auf ein Backup-Laufwerk oder die Verwendung umständlicher Backup-Software. Wurden diese recht lästigen Aufgaben vernachlässigt, so konnten bei einem Ausfall der Festplatte die Daten oft nur teilweise und nur mit hohem Zeit- und Kostenaufwand wiederhergestellt werden. Benutzer von Servern und Desktop-Computern dagegen genießen schon seit längerer Zeit die Sicherheit und Vorteile der RAID-Technologie (Redundant Array of Independent Disks) zur Wiederherstellung von Daten bei Festplattenausfällen.

HP bietet jetzt eine einfache RAID-Lösung für Notebookbenutzer an, die Daten auf ihren SATA-Festplatten gegen Festplattenausfall oder Virenangriffe schützen möchten. Die RAID-Lösung von HP ist auch für solche Computerbenutzer von Vorteil, die häufig mit großen Dateien arbeiten und die Speicherleistung ihres Computers verbessern möchten.

HINWEIS: Die Abbildungen in diesem Handbuch liegen nur in englischer Sprache vor.

2 Überblick über die RAID-Technologie

In diesem Kapitel werden die in diesem Handbuch verwendeten Begriffe definiert und die von ausgewählten HP Business-Computern unterstützten RAID-Technologien beschrieben.

RAID-Terminologie

Einige der Begriffe in der folgenden Tabelle haben außer der beschriebenen noch weitere Bedeutungen, wir beschränken uns in diesem Handbuch aber auf den Bedeutungsumfang im Zusammenhang mit den beschriebenen RAID-Anwendungen.

Begriff	**Definition**
Fehlertoleranz	Die Fähigkeit des Computers weiterzuarbeiten, wenn eine Festplatte ausfällt. Fehlertoleranz wird oftmals synonym mit Zuverlässigkeit verwendet, aber es besteht ein Unterschied.
Festplatte	Einer der physikalisch separaten Datenträger im RAID-Array. Im Zusammenhang mit RAID spricht man auch von „Laufwerk“ und meint damit ein physikalisches Festplattenlaufwerk.
Options-ROM	Ein Softwaremodul innerhalb des System-BIOS, das eine erweiterte Unterstützung für einen bestimmten Hardwarebaustein bietet. Das RAID-Options-ROM bietet Bootunterstützung für RAID-Volumes sowie eine Benutzerschnittstelle zum Verwalten und Konfigurieren der RAID-Volumes des Systems.
Primäres Laufwerk	Die interne Hauptfestplatte im Computer.
RAID-Array	Die physikalischen Laufwerke, die dem Betriebssystem zusammen als ein logisches Laufwerk dargestellt werden.
RAID-Migration	Die Änderung des Datenspeichers von einer Nicht-RAID-Konfiguration in eine RAID-Konfiguration. Die Migration der RAID-Ebene, d. h. die Änderung des Datenspeichers von einer RAID-Ebene auf eine andere, wird nicht unterstützt.
RAID-Volume	Eine festgelegte Menge Datenspeicher auf einem RAID-Array, das dem Betriebssystem als einzelne Festplatte dargestellt wird.
Wiederherstellungslaufwerk	Diejenige Festplatte, die in einem RAID 1- oder Recovery-Volume als Spiegel (Kopie des primären Laufwerks) bestimmt ist.
Zuverlässigkeit	Die Wahrscheinlichkeit, dass eine Festplatte innerhalb eines bestimmten Zeitraums ohne Fehler funktioniert. Wird auch als durchschnittliche fehlerfreie Betriebszeit (MTBF, mean time before failure) bezeichnet.
Stripe	Der Datenblock auf einer einzelnen Festplatte in einem RAID-Volume.
Striping	Die Verteilung von Daten über mehrere Festplattenlaufwerke zum Zwecke der Verbesserung der Lese-/Schreibleistung.

Unterstützte RAID-Modi

Zu den von HP Business-Computern unterstützten RAID-Modi gehören RAID 0, RAID 1, RAID 5 und flexibler Datenschutz (Recovery). Diese Modi werden im Folgenden beschrieben. Für RAID 0, RAID 1 und Recovery sind zwei SATA-Festplatten erforderlich. Für den Modus RAID 5 sind drei SATA-Festplatten erforderlich. Die hierfür benötigte zweite SATA-Festplatte kann im Erweiterungsschacht, am eSATA-Anschluss (wenn vorhanden), im zweiten Festplattenschacht (wenn vorhanden) oder im Schacht für SATA-Wechsellaufwerke der HP Advanced Docking Station installiert werden (siehe „Unterstützte Geräte“ auf Seite 7). RAID 10 wird nicht unterstützt.

RAID 0

Bei RAID 0 werden die Daten über die beiden Laufwerke verteilt (Striping). Dadurch können die Daten, insbesondere große Dateien, schneller gelesen werden, weil die Daten gleichzeitig von beiden Laufwerken gelesen werden. RAID 0 bietet jedoch keinerlei Fehlertoleranz: Fällt ein Laufwerk aus, ist das gesamte Array außer Funktion.

Die nutzbare Größe der Laufwerke ist der kleinste nicht zugeordnete Speicherplatz x 2 (Anzahl der Festplatten). Beispiel: Wenn Festplatte 1 über 150 GB freien Speicherplatz und Festplatte 2 über 600 GB freien Speicherplatz verfügt, beträgt die nutzbare Größe 150 x 2 = 300 GB. Es wird empfohlen, Festplatten mit derselben Größe und denselben Spezifikationen für die RAID-Konfiguration zu verwenden.

RAID 1

Bei RAID 1 werden die Daten in identischer Form auf beide Festplatten kopiert (Spiegelung). Fällt eine Festplatte aus, können die Daten von der anderen Festplatte wiederhergestellt werden.

Die nutzbare Größe der Laufwerke ist der kleinste nicht zugeordnete Speicherplatz. Beispiel: Wenn Festplatte 1 über 150 GB freien Speicherplatz und Festplatte 2 über 600 GB freien Speicherplatz verfügt, beträgt die nutzbare Größe 150 GB. Es wird empfohlen, Festplatten mit derselben Größe und denselben Spezifikationen für RAID zu verwenden.

RAID 5

RAID 5 verteilt Daten über drei Festplatten. Fällt eine Festplatte aus, können die Daten mit RAID 5 von den anderen beiden Festplatte wiederhergestellt werden.

Die nutzbare Größe der Laufwerke ist der kleinste nicht zugeordnete Speicherplatz x 3 (Anzahl der Festplatten) x 2/3. Beispiel: Wenn Festplatte 1 über 150 GB freien Speicherplatz, Festplatte 2 über 600 GB freien Speicherplatz und Festplatte 3 über 400 GB freien Speicherplatz verfügt, beträgt die nutzbare Größe 300 GB (150 GB x 3 x 2/3). Es wird empfohlen, Festplatten mit derselben Größe und denselben Spezifikationen für RAID zu verwenden.

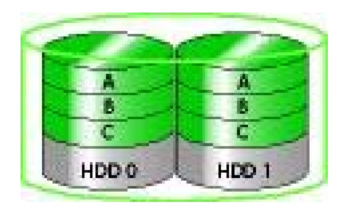
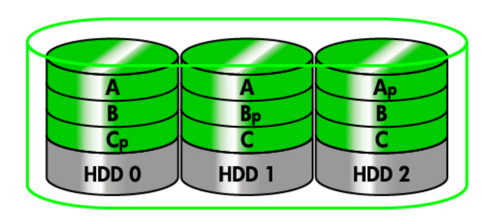
Flexibler Datenschutz (Recovery)

Flexibler Datenschutz (Recovery) ist ein Merkmal der Intel® Rapid Storage Technology Software. Recovery erweitert die Funktionalität von RAID 1 um mehrere Merkmale, die dem Benutzer das Spiegeln der Daten auf ein bestimmtes Wiederherstellungslaufwerk erleichtern. Mit Recovery kann der Benutzer beispielsweise festlegen, wie das Recovery-Volume aktualisiert wird: ständig (Standardeinstellung) oder auf Anforderung. Recovery ermöglicht außerdem das An- und Abdocken des Computers, wenn sich das zweite Laufwerk im Schacht der Dockingstation befindet.

Überblick über die RAID-Modi

In der folgenden Tabelle werden die Funktionen, Anwendungen sowie Vor- und Nachteile der unterstützten RAID-Modi beschrieben.

RAID-Ebenen	Funktion/Anwendungen	Vorteile/Nachteile
RAID 0	**Funktion:** **Die Daten werden über beide Festplatten verteilt.** Anwendungen: ● Bildbearbeitung ● Videoproduktion ● Druckvorbereitung	**Vorteile:** **Die Leseleistung ist höher als bei Nicht-RAID-Festplatten.** **Die Speicherkapazität wird verdoppelt.** Nachteile: Wenn eine Festplatte ausfällt, ist das gesamte Array außer Funktion. Die Daten können nicht wiederhergestellt werden. Wenn die Kapazitäten des primären und sekundären Laufwerks unterschiedlich sind, kann Speicherkapazität verloren gehen (siehe „HP SATA Laufwerk-Optionskits“ auf Seite 8).
RAID 1	**Funktion:** **Identische (gespiegelte) Daten werden auf zwei Laufwerken gespeichert.** Anwendungen: ● Buchhaltung ● Lohnbuchhaltung ● Finanzen	**Vorteile:** **Bietet eine hohe Fehlertoleranz.** Nachteile: Nur die Hälfte der Gesamtspeicherkapazität kann für die Datenspeicherung verwendet werden. Wenn die Kapazitäten des primären und sekundären Laufwerks unterschiedlich sind, kann Speicherkapazität verloren gehen (siehe „HP SATA Laufwerk-Optionskits“ auf Seite 8).

RAID-Ebenen	Funktion/Anwendungen	Vorteile/Nachteile
RAID Recovery 	**Funktion:** **Identische (gespiegelte) Daten werden auf zwei Laufwerken gespeichert.** **Die Funktionalität von RAID 1 wird um nützliche Funktionen erweitert.** Anwendungen: Jede Anwendung, in der eine einfache Datenschutz-methode benötigt wird.	**Vorteile:** **Bietet eine hohe Fehlertoleranz.** **Der Benutzer kann festlegen, ob die Daten ständig oder nur auf Anforderung gespiegelt werden.** **Daten- wiederherstellung ist schnell und einfach.** **Ermöglicht das Anschließen und Trennen des Spiegellaufwerks während des Betriebs (Hot-Plugging), wenn es sich am eSATA-Anschluss oder in der Dockingstation befindet.** **Erlaubt eine einfache Migration auf Nicht-RAID.** Nachteile: Nur die Hälfte der Gesamtspeicherkapazität kann für die Datenspeicherung verwendet werden. Wenn die Kapazitäten des primären und sekundären Laufwerks unterschiedlich sind, kann Speicherkapazität verloren gehen.
RAID 5 	**Funktion:** Verteilt Daten über drei Festplatten. Fällt eine Festplatte aus, können die Daten mit RAID 5 von den anderen beiden Festplatten wiederhergestellt werden. Anwendungen: Eine gute Wahl, wenn große Mengen wichtiger Daten vorhanden sind.	**Vorteile:** **Datenredundanz** **Verbesserte Leistung und Kapazität** **Hohe Fehlertoleranz und Leseleistung** Nachteile: Während einer RAID-Wiederherstellung nach einem Festplattenausfall verringert sich die Systemleistung möglicherweise.

Die Vorteile der unterstützten RAID-Modi

Fehlertoleranz und Leistung sind für die Wahl eines RAID-Modus die wichtigsten Grundbegriffe.

Fehlertoleranz

Fehlertoleranz ist die Fähigkeit eines RAID-Arrays, den Betrieb bei einem Festplattenausfall fortzusetzen und die Daten wiederherzustellen. Fehlertoleranz wird durch Redundanz ermöglicht. RAID 0 hat demnach keine Fehlertoleranz, weil keine Daten auf eine andere Festplatte kopiert werden. Bei RAID 1 und Recovery kann ein Laufwerk ausfallen, ohne dass das gesamte Array ausfällt. Mit Recovery ist jedoch die Wiederherstellung einer einzelnen Datei oder der gesamten Festplatte einfacher als mit RAID 1 allein. Bei RAID 5 kann eine der drei Festplatten ausfallen, ohne dass das gesamte Array ausfällt.

Leistung

Die Leistung eines Festplattenarrays ist schwierig zu messen, weil mehrere Faktoren berücksichtigt werden müssen. Eine Erläuterung all dieser Faktoren liegt außerhalb des Rahmens dieses Dokuments. Die gesamte Speicherleistung wird durch die Schreibleistung und die Leseleistung bestimmt. Beide sind je nach gewählter RAID-Technologie unterschiedlich.

- RAID 0 (Striping) verbessert die Gesamt-Speicherleistung, da die Daten auf zwei Festplatten gleichzeitig geschrieben und gelesen werden können.
- Recovery und RAID 1 (Spiegeln) schreiben dieselben Daten auf beide Festplatten; aus diesem Grund kann sich die Schreibleistung verringern. Da die Daten jedoch von beiden Festplatten gelesen werden können, kann die Leseleistung besser sein als bei einer einzelnen Nicht-RAID-Festplatte.
- RAID 5 umfasst die Leistungsmerkmale von RAID 0 und RAID 1.

3 Unterstützte Betriebssysteme und Geräte

Unterstützte Betriebssysteme

HP RAID unterstützt 32-Bit- und 64-Bit-Versionen der Betriebssysteme Windows Vista® (SP1 und SP2) und Windows 7.

HINWEIS: HP bietet nur eingeschränkte Unterstützung für Microsoft® Windows® XP Professional (SP1, SP2 und SP3).

Unterstützte Geräte

In diesem Abschnitt wird beschrieben, welche Geräte, einschließlich SATA-Laufwerke, Computer und Dockingstation, für die RAID-Migration unterstützt werden. Die unterstützten Geräte werden in der folgenden Tabelle zusammengefasst und danach detailliert beschrieben. Externe SATA-Laufwerke, die über USB mit dem Computer oder der Dockingstation verbunden sind, können nicht nach RAID migriert werden.

	Interne primäre SATA-Festplatte und SATA-Festplatte im Erweiterungsschacht	SATA-Festplatten im primären und sekundären Festplattenschacht im Computer	Festplatte in der Dockingstation oder über eSATA angeschlossene Festplatte
RAID 0	Ja	Ja	Nein
RAID 1	Ja	Ja	Nein
Recovery	Ja	Ja	Ja
RAID 5	Ja	Ja	Nein

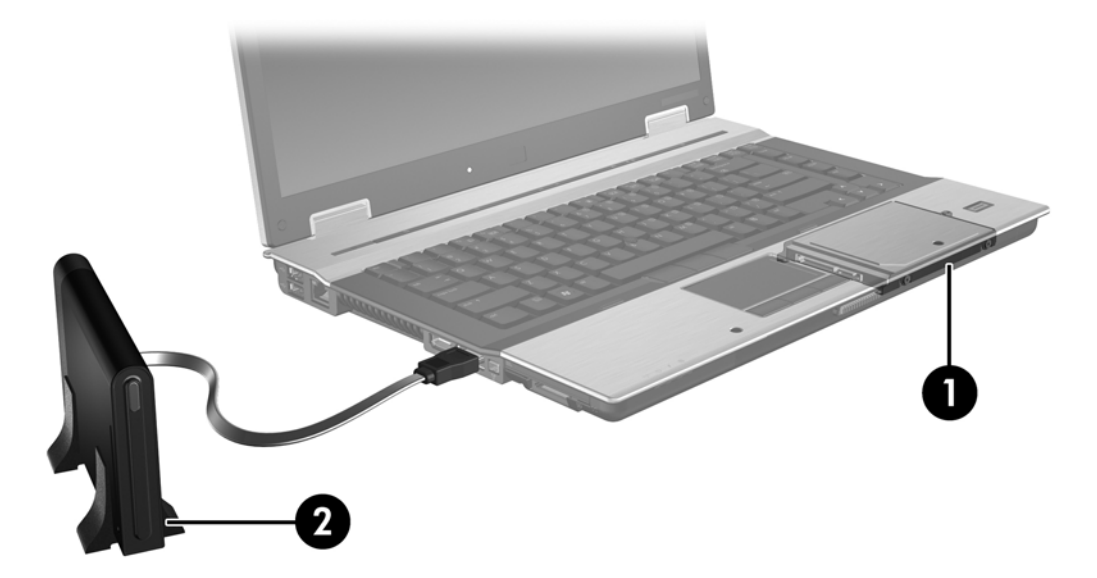
HP SATA Laufwerk-Optionskits

Zur Unterstützung der RAID-Migration bietet HP SATA-Laufwerk-Optionskits für den Erweiterungsschacht des Computers und den Schacht für SATA-Wechsellaufwerke der Dockingstation. Für eine optimale RAID-Leistung wird empfohlen, dass beide Laufwerke über dieselbe Geschwindigkeit verfügen. Unterstützte HP Business-Computer erlauben jedoch auch die Verwendung von Laufwerken unterschiedlicher Geschwindigkeiten in einem RAID-Volume.

Auch Laufwerke mit verschiedenen Kapazitäten werden unterstützt, sofern die Kapazität des sekundären Laufwerks (Wiederherstellungslaufwerks) nicht kleiner ist als die des primären Laufwerks. Verfügt das primäre Laufwerk beispielsweise über 200 GB, so muss im Erweiterungsschacht ein Laufwerk mit mindestens 200 GB installiert sein, um ein RAID-Volume zu erstellen. Ist die Kapazität des sekundären Laufwerks größer als die des primären, kann die Überkapazität des sekundären (oder tertiären) Laufwerks nicht genutzt werden. Ist das primäre Laufwerk beispielsweise 160 GB groß und das sekundäre 250 GB, können in einer RAID-Konfiguration nur 160 GB des sekundären Laufwerks genutzt werden. Für eine optimale Nutzung wird deshalb empfohlen, dass beide Laufwerke über dieselbe Kapazität verfügen.

eSATA-Festplatten (bestimmte Modelle)

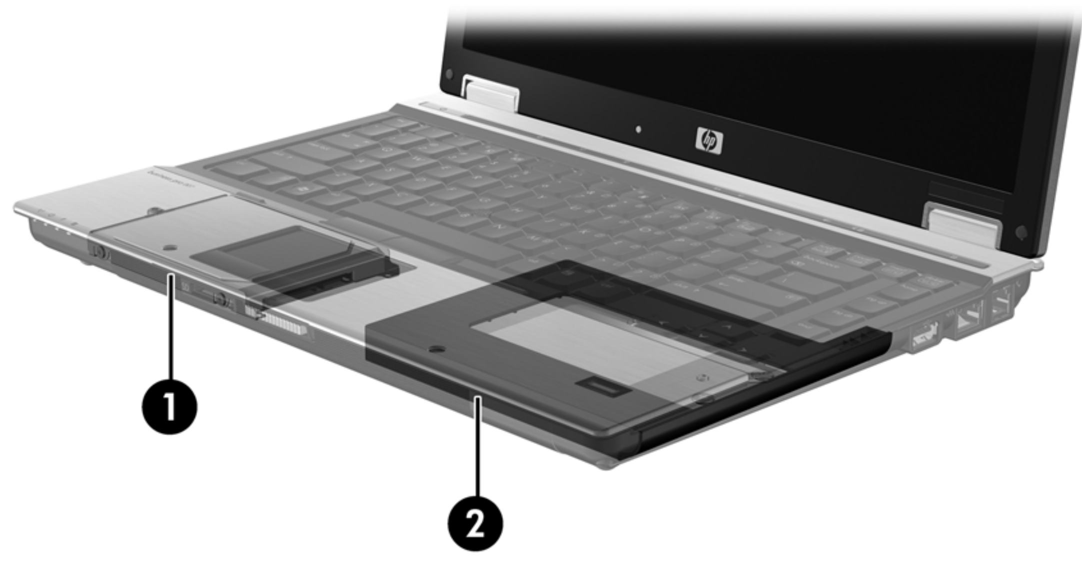
Externes SATA, oder eSATA, ist eine externe Schnittstelle für SATA-Laufwerke, die eine Datenübertragung mit bis zu 6-mal schnellerer Geschwindigkeit ermöglicht als über eine Standard-USB 2.0-Schnittstelle. Die folgende Abbildung zeigt einen unterstützten Computer mit einer primären Festplatte **(1)** und einem am eSATA-Anschluss angeschlossenen eSATA-Laufwerk **(2)** (bestimmte Modelle). Diese Konfiguration unterstützt Recovery. Für die Kapazität des eSATA-Laufwerks gelten dieselben Empfehlungen wie bei sekundären Laufwerken im Erweiterungsschacht des Computers.



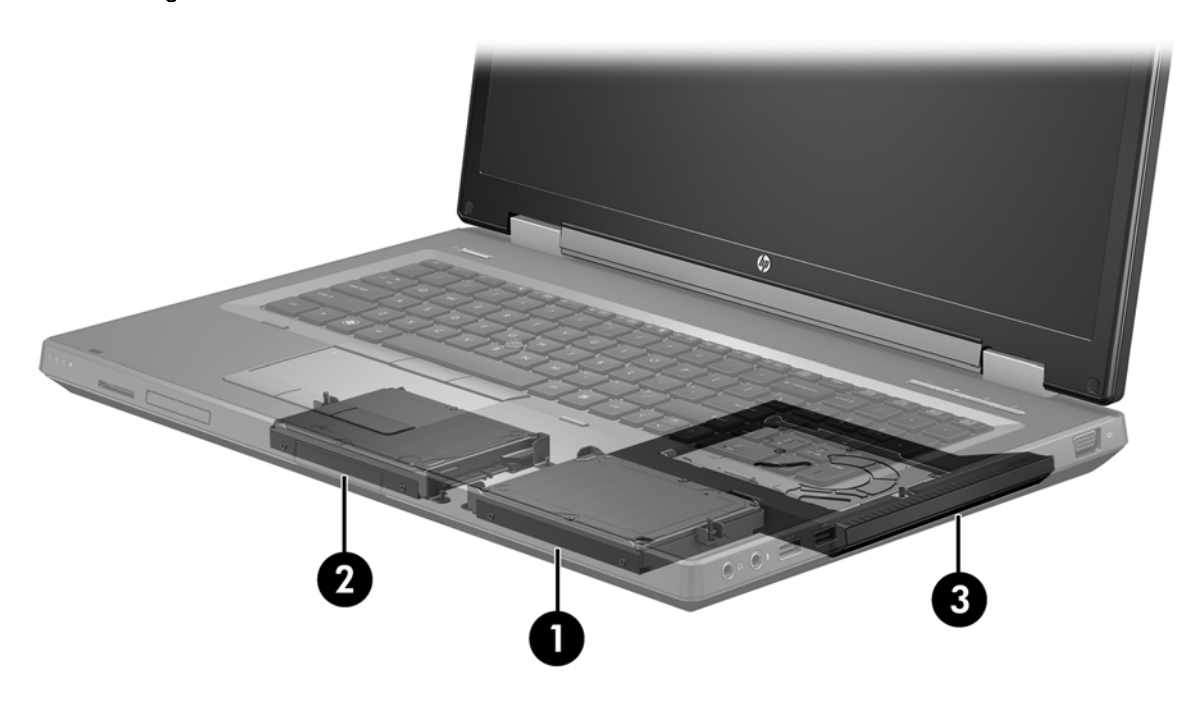
HP Business-Computer

Ausgewählte HP Business-Computer unterstützen RAID mithilfe der Intel® Rapid Storage Technology Software (ab v10) und einem sekundären SATA-Laufwerk im Erweiterungsschacht.

Die folgende Abbildung zeigt einen unterstützten Computer mit der primären Festplatte **(1)** und einer sekundären SATA-Festplatte im Erweiterungsschacht **(2)**. Diese Konfiguration unterstützt RAID 0, RAID 1 und Recovery.



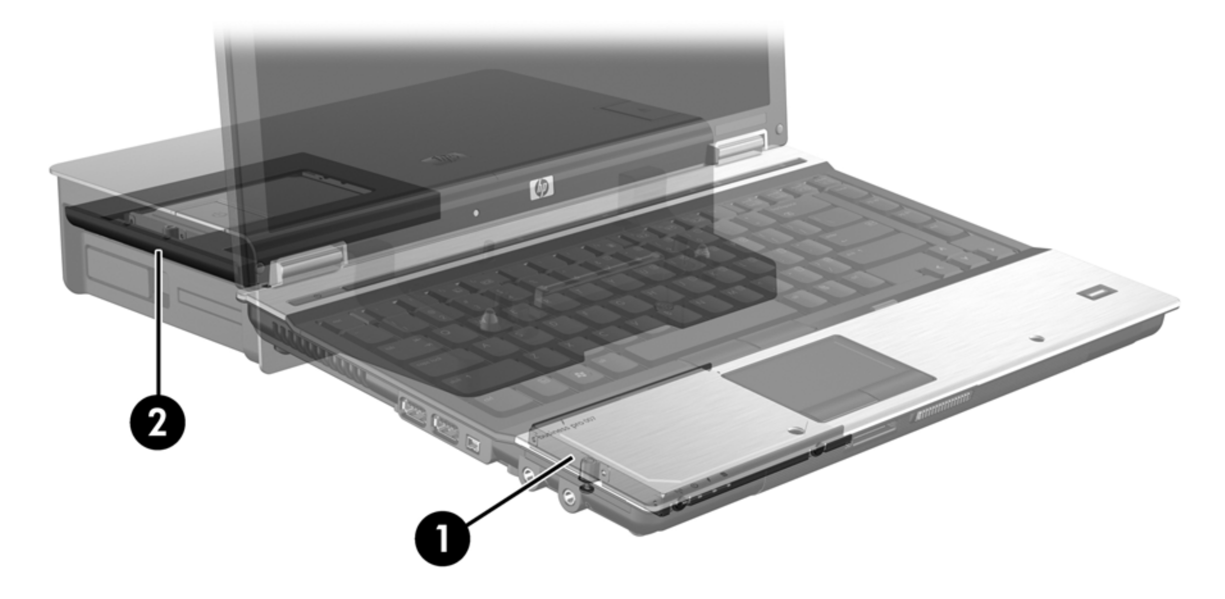
Die folgende Abbildung zeigt einen unterstützten Computer mit der primären Festplatte **(1)** und einer sekundären Festplatte **(2)**, während sich das tertiäre Laufwerk im Erweiterungsschacht befindet **(3)**. Diese Konfiguration unterstützt RAID 5.



HP Advanced Docking Station

Recovery unterstützt das An- und Abdocken. Mithilfe dieser Technologie kann die Spiegelung zwischen der primären Festplatte **(1)** und einer optionalen Festplatte im Schacht für SATA-Wechsellaufwerke der HP Advanced Docking Station **(2)** implementiert werden.

Die folgende Abbildung zeigt eine HP Advanced Docking Station mit der Wiederherstellungsfestplatte im Schacht für SATA-Wechsellaufwerke. Diese Konfiguration unterstützt Recovery.



4 Merkmale der Intel Rapid Storage Technology

Die Intel Rapid Storage Technology unterstützt die folgenden Recovery-Merkmale.

Advanced Host Controller Interface

Advanced Host Controller Interface (AHCI) ist eine Spezifikation, die dem Speichertreiber die Verwendung erweiterter SATA-Merkmale wie Native Command Queuing und Hot-Plug-Funktionalität ermöglicht. AHCI muss im System-BIOS aktiviert sein, um diese Merkmale nutzen zu können (siehe „Aktivieren von RAID im System-BIOS (f10)“ auf Seite 14). Auf unterstützten HP Business-Computern ist AHCI standardmäßig aktiviert.

Native Command Queuing

In Abhängigkeit von der Reihenfolge des Eingangs der Schreibanfrage schreibt ein Schreib-/Lesekopf die Daten in konzentrischen Kreisen (Spuren) auf eine Festplatte. Da die Anwendungen die Daten jedoch selten in derselben Reihenfolge wieder abfragen, in der sie auf die Platte geschrieben wurden, käme es zu langen Verzögerungen (Latenzzeiten), wenn der Laufwerkskopf die Daten in genau derselben Reihenfolge aufsuchen würde, in der die Leseanfragen eingehen. Die Technologie Native Command Queuing (NCQ) ermöglicht es SATA-Festplatten, mehrere Befehle anzunehmen und in einer anderen Reihenfolge auszuführen, um so eine schnellere Leseleistung zu erzielen. Der Vorgang ist vergleichbar mit einem Aufzug, der die angeforderten Stockwerke in einer logischeren Reihenfolge abarbeitet, um Fahrzeiten und Verschleiß zu minimieren. NCQ verringert auf ganz ähnliche Weise beim Abarbeiten mehrerer Schreib-/Leseanforderungen die Latenzzeiten und die vom Laufwerkskopf zurückzulegenden Wege. Dadurch steigen Leistung und Zuverlässigkeit. NCQ muss vom System-BIOS, vom SATA-Controller und vom Controllertreiber unterstützt werden.

Hot-Plug-Funktionalität

Die Hot-Plug-Funktionalität ermöglicht ein Trennen oder Anschließen bzw. Einsetzen der SATA-Wiederherstellungsfestplatte, während der Computer in Betrieb ist. Die Hot-Plug-Funktionalität wird unterstützt, wenn die Wiederherstellungsfestplatte am eSATA-Anschluss angeschlossen ist oder sich im Schacht für SATA-Wechsellaufwerke der Dockingstation befindet. So kann beispielsweise die Wiederherstellungsfestplatte bei laufendem Computer aus dem Schacht für SATA-Wechsellaufwerke entnommen werden, wenn Sie vorübergehend ein optisches Laufwerk in den Schacht einsetzen möchten. Dank der Hot-Plug-Funktionalität können Sie den Computer auch jederzeit an- oder abdocken.

Intel Rapid Recover Technology

Die Intel Rapid Storage Technology unterstützt die folgenden Recovery-Merkmale.

Vorgehensweisen zum Aktualisieren des Spiegellaufwerks

Mit Recovery können Sie selbst festlegen, wie oft die Wiederherstellungsfestplatte aktualisiert wird: ständig oder auf Anforderung. Bei ständiger Aktualisierung werden die Daten auf dem primären Laufwerk stets gleichzeitig auch auf das Spiegellaufwerk kopiert, solange beide Laufwerke mit dem System verbunden sind. Wenn Sie den Computer von der Dockingstation trennen, in der sich das Wiederherstellungslaufwerk befindet, werden alle neuen oder geänderten Daten automatisch von der primären Festplatte auf die Wiederherstellungsfestplatte kopiert, sobald das Notebook wieder angedockt wird. Dabei kann auch ein Spiegelungsvorgang fortgesetzt werden, der beim Abdocken unterbrochen wurde.

Bei Aktualisierung auf Anforderung werden die Daten nur dann von der primären Festplatte auf die gespiegelte Festplatte kopiert, wenn dies durch den Befehl **Update Recovery Volume** (Recovery-Volume aktualisieren) in Recovery angefordert wird. Dabei werden nur die neuen oder aktualisierten Dateien vom primären Laufwerk auf die Wiederherstellungsfestplatte kopiert. Vor der Aktualisierung der gespiegelten Festplatte können bei dieser Vorgehensweise auch einzelne Dateien wiederhergestellt werden, die auf der primären Festplatte beschädigt wurden. Durch Aktualisierung nur auf Anforderung können Sie die Daten auf der gespiegelten Festplatte auch vor einem eventuellen Virenbefall der primären Festplatte schützen. Dazu darf die gespiegelte Festplatte nach dem Virenbefall allerdings nicht aktualisiert werden.

HINWEIS: Die Aktualisierungsweise des Spiegellaufwerks können Sie jederzeit ändern. Klicken Sie hierzu mit der rechten Maustaste auf **Modify Volume Update Policy** (Aktualisierungsweise für Volume ändern).

Automatische Umschaltung zwischen Festplatten und schnelle Wiederherstellung

Wenn die primäre Festplatte ausfällt, schaltet Recovery ohne Eingriff des Benutzers auf das gespiegelte Laufwerk um. Recovery meldet den Ausfall der primären Festplatte. In der Zwischenzeit kann der Computer von der gespiegelten Festplatte starten. Wenn eine neue primäre Festplatte installiert wird und der Computer neu gestartet wird, kopiert die schnelle Wiederherstellungsfunktion von Recovery alle gespiegelten Daten zurück auf die primäre Festplatte.

HINWEIS: Wurde die Einstellung „Aktualisierung auf Anforderung" ausgewählt und das primäre Laufwerk fällt aus oder eine Datei auf dem primären Laufwerk wird beschädigt, gehen alle nicht gespiegelten Daten verloren.

Vereinfachte Migration von RAID auf Nicht-RAID

Um aus einem RAID 1- oder Recovery-Volume wieder zwei Nicht-RAID-Festplatten zu erstellen, gehen Sie nach der Anleitung im folgenden Abschnitt vor: „Zurücksetzen von RAID-Laufwerken auf Nicht-RAID" auf Seite 40.

Auch die Migration von RAID 1 nach Recovery wird unterstützt. Die Migration von RAID 0 nach RAID 1 oder von RAID 0 nach einer Nicht-RAID-Primärfestplatte wird jedoch nicht unterstützt.

5 Einrichtung des RAID-Volume

In den folgenden Anleitungen wird davon ausgegangen, dass eine unterstützte Festplatte im Erweiterungsschacht des Computers oder im Schacht für SATA-Wechsellaufwerke der Dockingstation installiert ist oder am eSATA-Anschluss des Computers angeschlossen ist (siehe „Unterstützte Geräte“ auf Seite 7).

Die RAID-Migration besteht im Prinzip aus den folgenden Schritten:

- RAID im System-BIOS aktivieren.
- RAID-Migration mithilfe der Intel® Rapid Storage Technology Console.

ACHTUNG: Stellen Sie sicher, dass der Computer an eine Netzstromquelle angeschlossen ist, bevor Sie mit den folgenden Vorgängen beginnen. Wenn bei einer RAID-Migration die Stromversorgung ausfällt, kann dies zu Datenverlust führen.

Aktivieren von RAID im System-BIOS (f10)

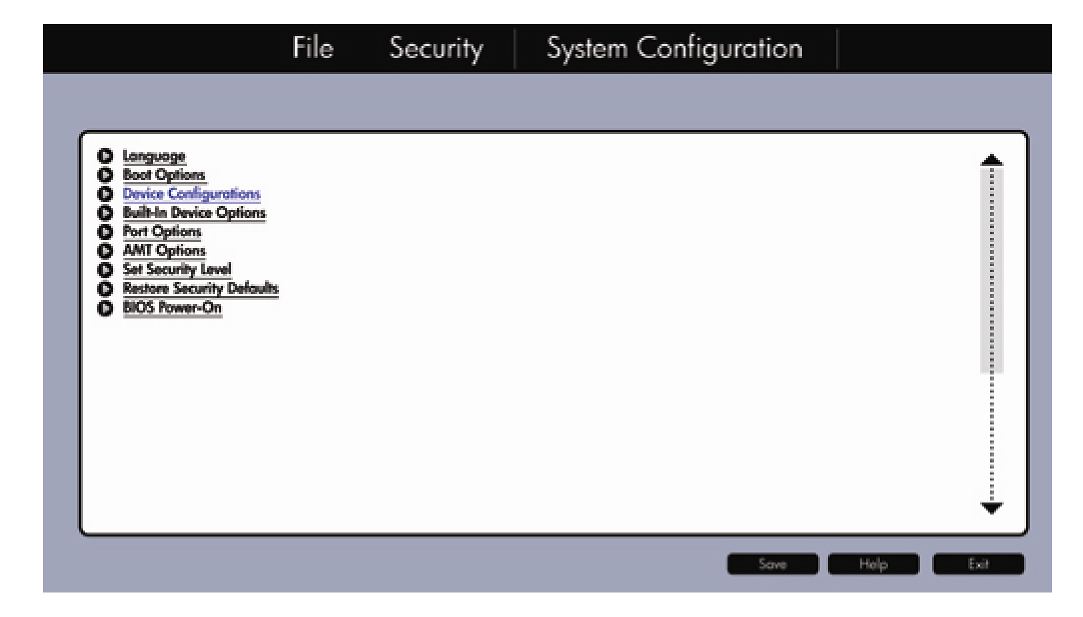
HINWEIS: In der folgenden Anleitung wird davon ausgegangen, dass Sie das Festplatten-Image verwenden, das mit dem Computer geliefert wurde. Wenn auf dem Computer ein anderes Image installiert ist, müssen Sie *zuerst* RAID im System-BIOS (f10), aktivieren und dann das Betriebssystem und alle erforderlichen Treiber installieren, auch den Treiber für die Intel Rapid Storage Technology. Folgen Sie dann der Anleitung unter „RAID-Migration mithilfe der Intel Rapid Storage Technology Console“ auf Seite 17.

Sie müssen die RAID-Funktionalität im System-BIOS aktivieren, um den SATA-Host Controller auf RAID umzuschalten. Führen Sie folgende Schritte aus:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
2. Drücken Sie sofort beim Hochfahren des Computers f10, um Computer Setup zu starten.

   HINWEIS: Wenn Sie die Taste f10 nicht rechtzeitig gedrückt haben, müssen Sie den Computer erneut starten und dann nochmals f10 drücken, um auf das Utility zuzugreifen.

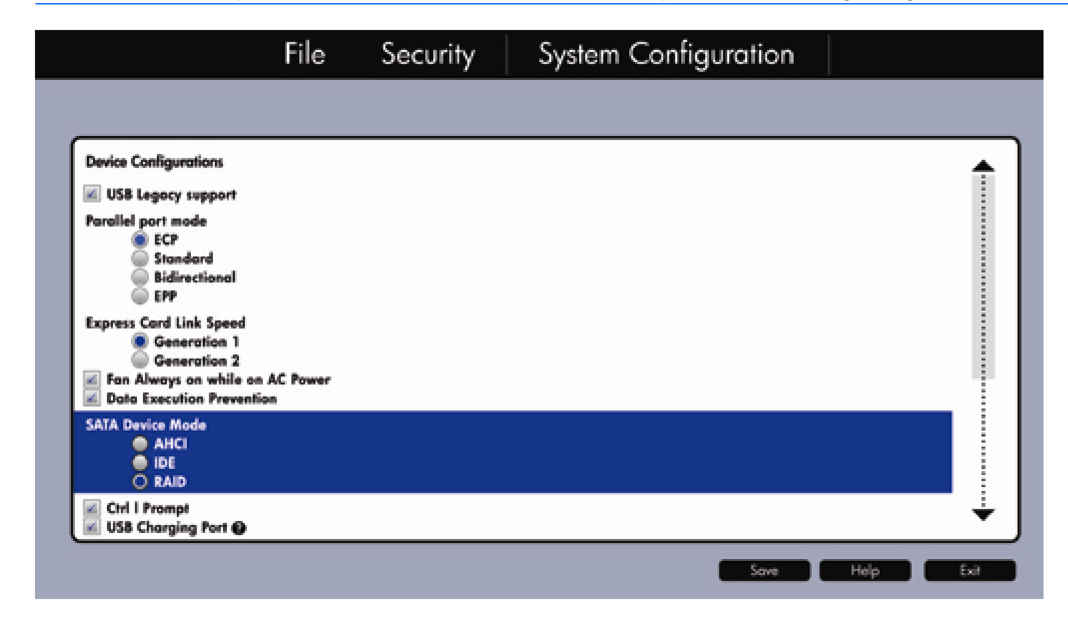
3. Wählen Sie im System-BIOS die Option **System Configuration** (Systemkonfiguration) **> Device Configurations** (Gerätekonfigurationen).



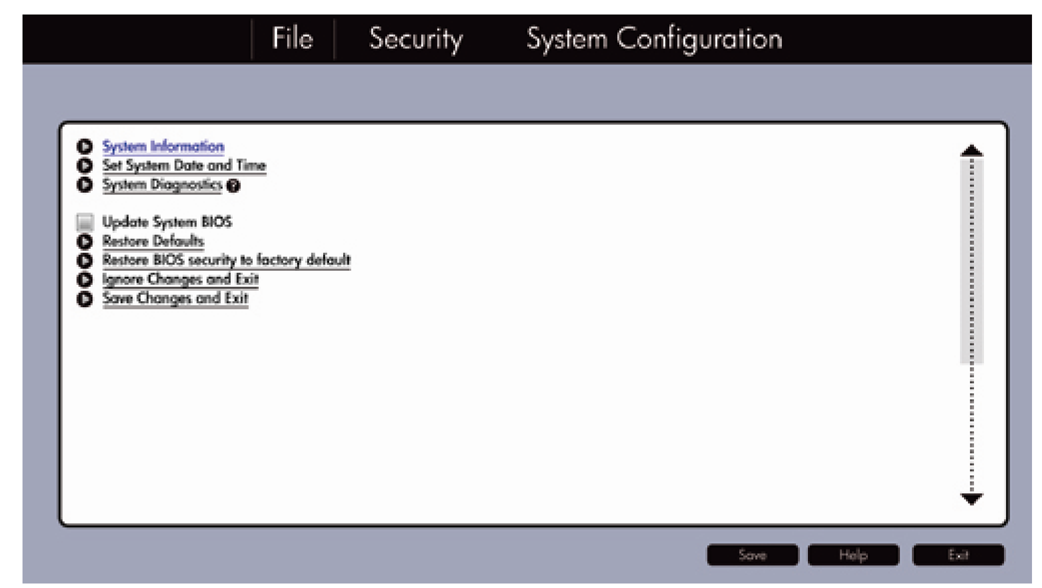
4. Wählen Sie im Fenster **Device Configurations** (Gerätekonfigurationen) unter **SATA Device Mode** (SATA-Gerätemodus) die Option **RAID** aus. Klicken Sie auf **Confirm** (Bestätigen). Folgende Meldung wird angezeigt: „Changing this setting may require reinstallation of your operating system. Are you sure you want to proceed?" (Wenn diese Einstellung geändert wird, ist möglicherweise eine erneute Installation Ihres Betriebssystems erforderlich. Möchten Sie wirklich fortfahren?)

HINWEIS: Das mit Ihrem Computer gelieferte Festplatten-Image enthält Treiber, die Ihnen ein Umschalten zwischen dem AHCI- und dem RAID-Modus ohne Neuinstallation des Betriebssystems ermöglichen. Wenn Sie ein anderes Festplatten-Image verwenden, müssen Sie möglicherweise das Betriebssystem neu installieren.

HINWEIS: Unter SATA Device Mode (SATA-Gerätemodus) befindet sich ein Kontrollkästchen für die <strg I>-Eingabeaufforderung. Wenn Sie dieses Kontrollkästchen aktivieren, wird beim Starten des Computers der Bildschirm für das Intel Options-ROM angezeigt.



5. Wählen Sie **File** (Datei) **> Save Changes and Exit** (Änderungen speichern und beenden). Klicken Sie dann auf **Yes** (Ja), um die Änderungen zu speichern. Wenn Sie die Änderungen doch nicht speichern möchten, wählen Sie **Ignore Changes and Exit** (Änderungen ignorieren und beenden).



ACHTUNG: Schalten Sie den Computer auf keinen Fall aus, während die in f10 Computer Setup vorgenommenen Änderungen im ROM gespeichert werden. Anderenfalls können die Daten im CMOS (Complementary Metal Oxide Semiconductor) beschädigt werden. Schalten Sie den Computer erst dann aus, wenn das mit f10 aufgerufene Computer Setup Utility geschlossen ist.

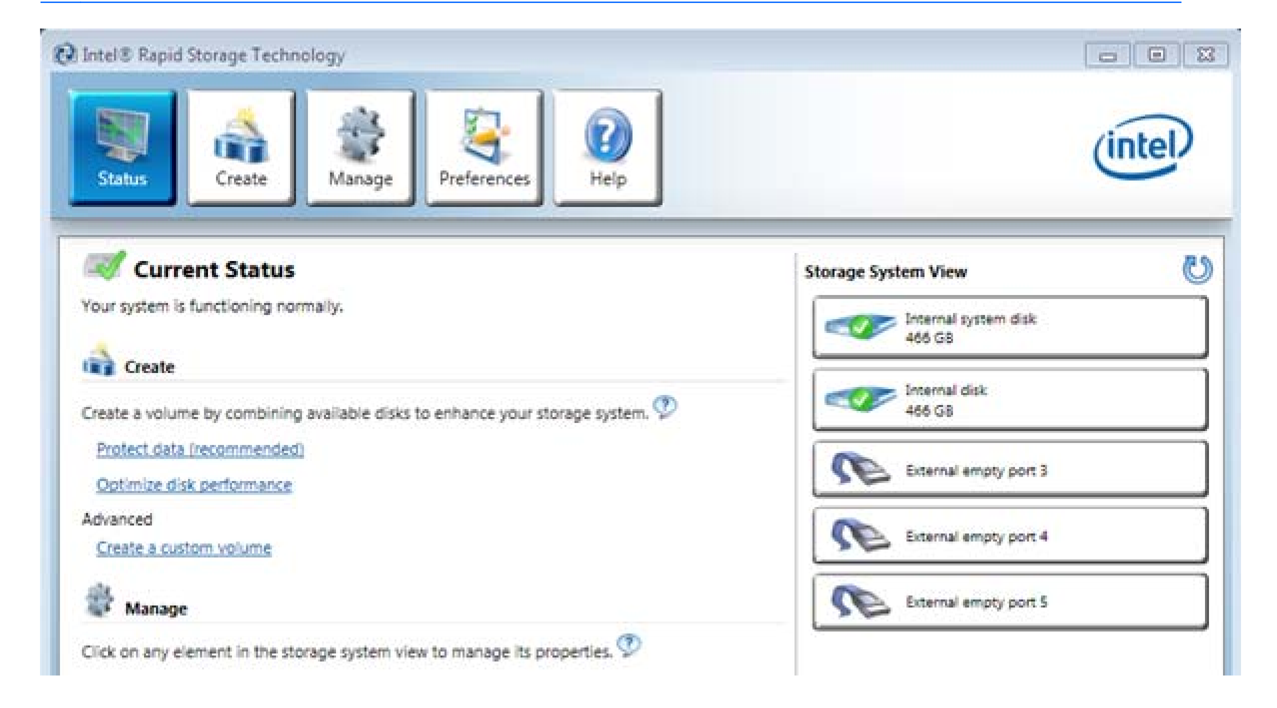
6. Nach dem Start des Betriebssystems können Sie mit der RAID-Migration beginnen.

RAID-Migration mithilfe der Intel Rapid Storage Technology Console

▲ Rufen Sie die Intel Rapid Storage Technology Console auf, indem Sie **Start > Alle Programme > Intel Rapid Storage Technology** wählen.

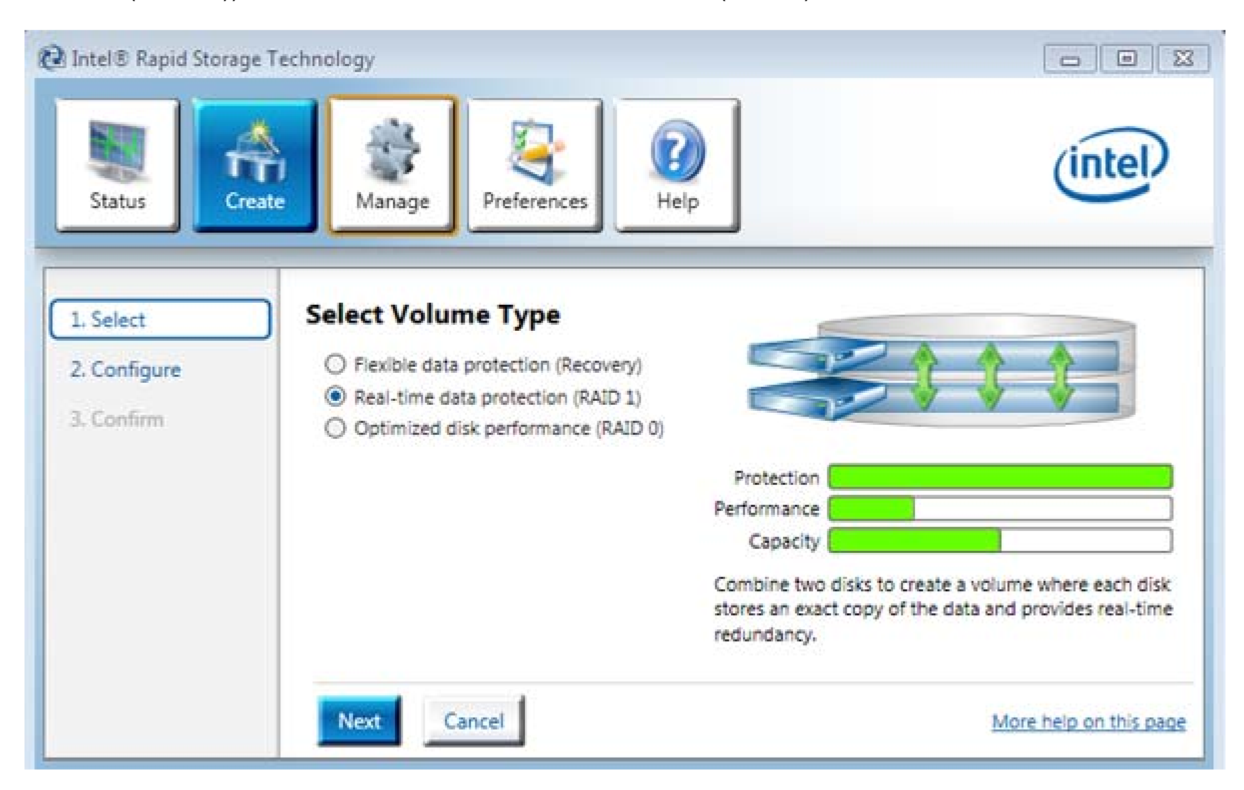
HINWEIS: In Windows Vista und Windows 7 ist das Merkmal Benutzerkontensteuerung zur Verbesserung der Sicherheit Ihres Computers enthalten. Sie werden möglicherweise aufgefordert, Ihre Erlaubnis zu erteilen bzw. ein Kennwort einzugeben, wenn Sie beispielsweise Software installieren, Dienstprogramme ausführen oder Windows Einstellungen ändern möchten. Weitere Informationen hierzu finden Sie unter Hilfe und Support.

Die Konsole startet mit dem Status-Bildschirm, der den aktuellen Status und die im System vorhandenen Festplatten anzeigt.

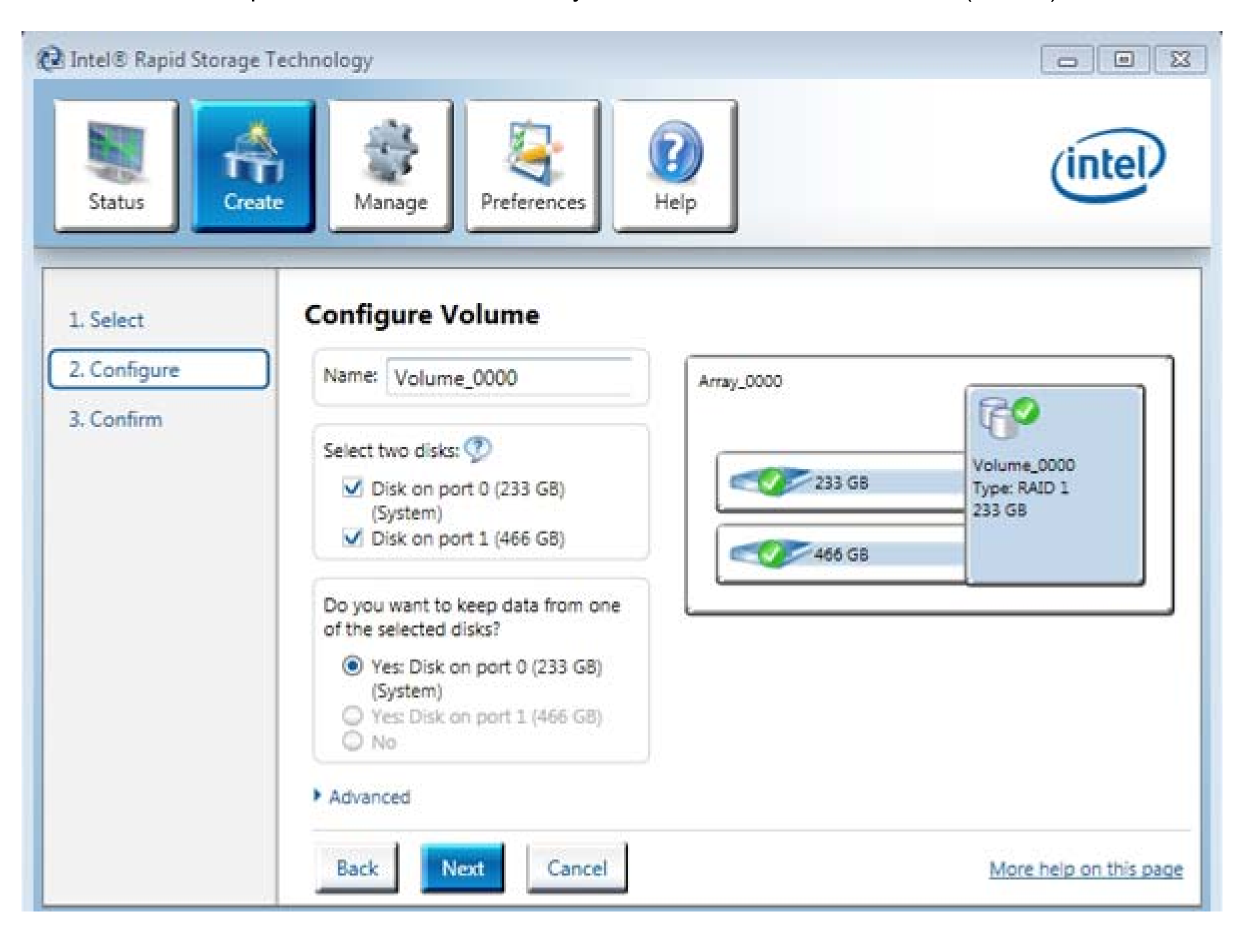


Migration auf RAID 1

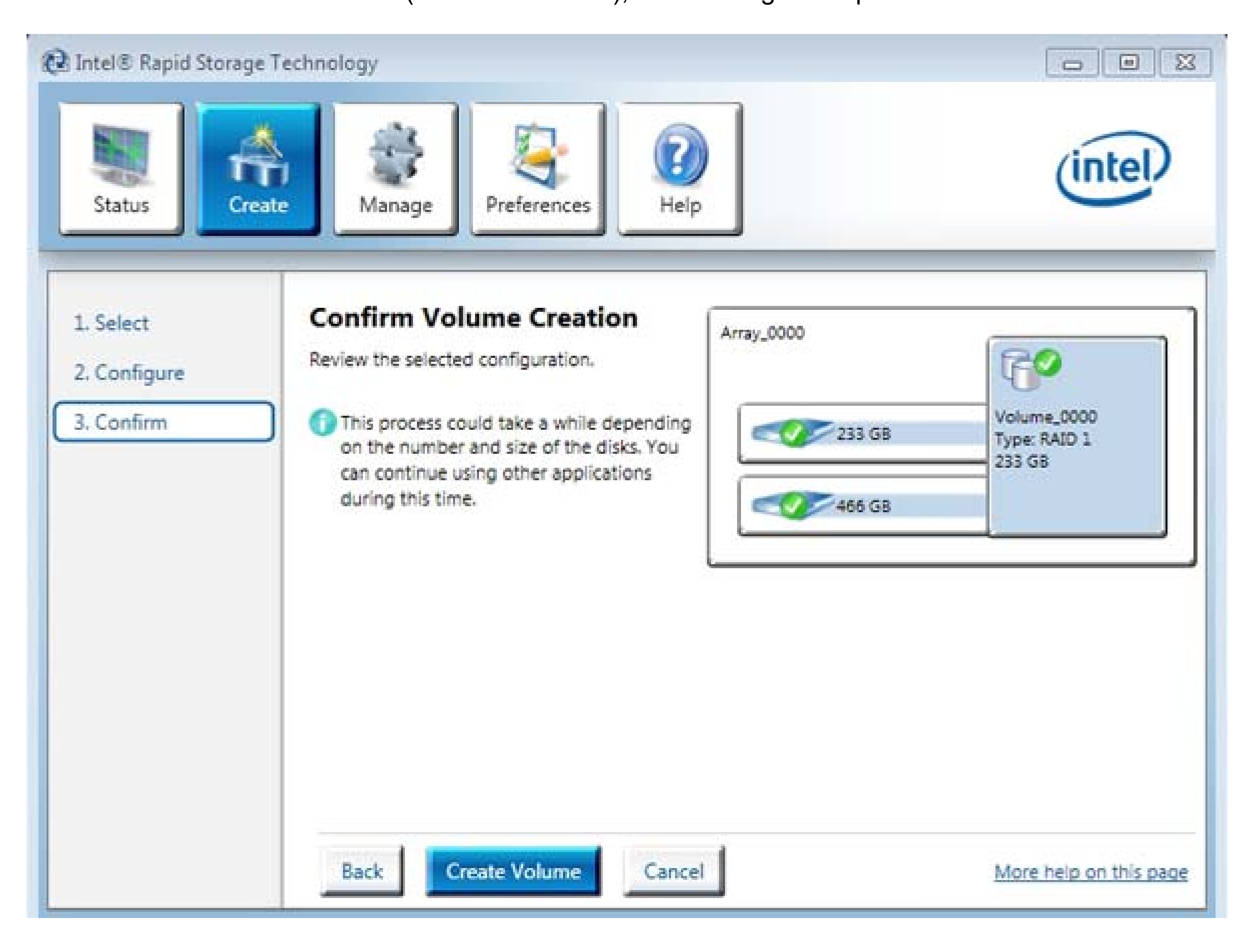
1. Klicken Sie auf **Create** (Erstellen), auf **Real-time data protection (RAID 1)** (Datenschutz in Echtzeit (RAID 1)), und klicken Sie anschließend auf **Next** (Weiter).



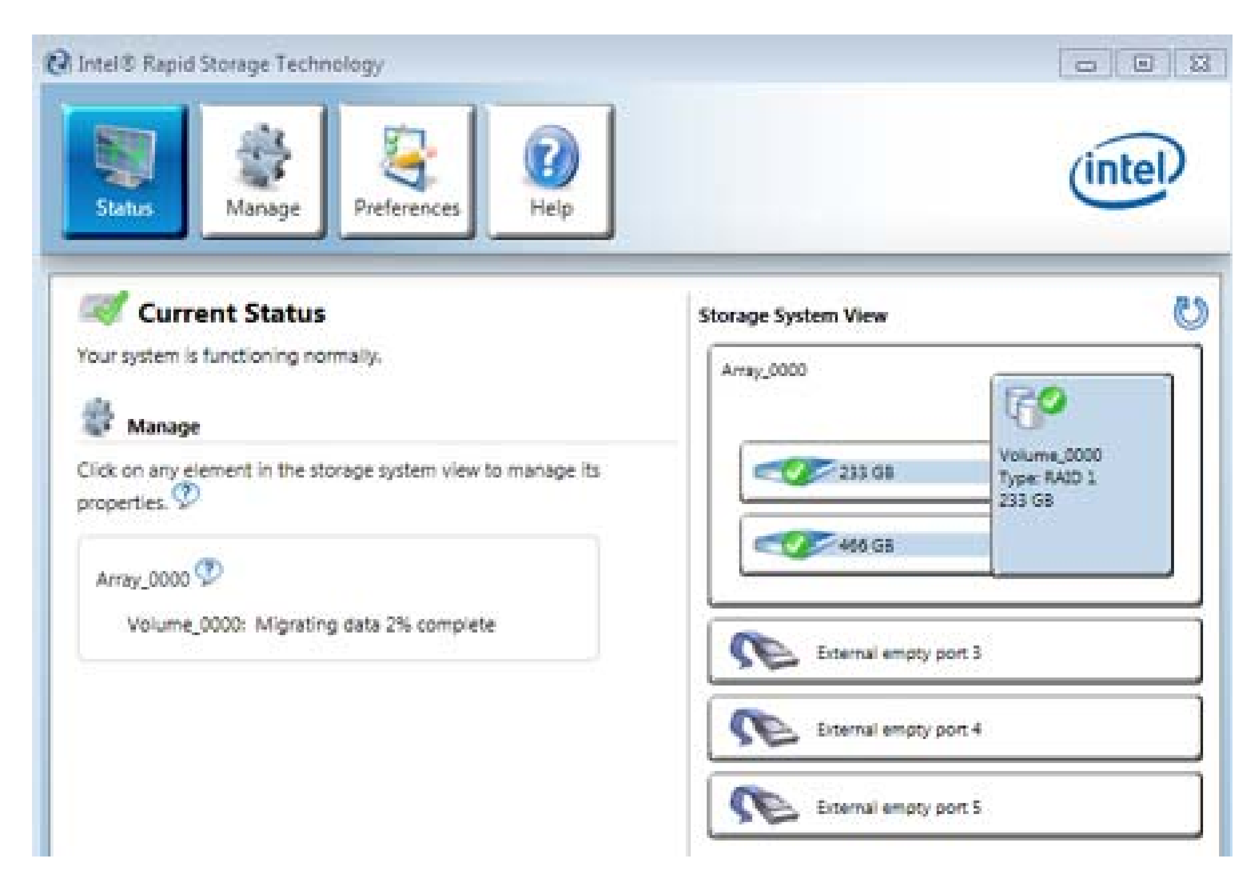
2. Erstellen Sie einen Volume-Namen (oder verwenden Sie den vorgeschlagenen Namen), wählen Sie die beiden Festplatten für das RAID 1-Array, und klicken Sie dann auf **Next** (Weiter).



3. Klicken Sie auf **Create Volume** (Volume erstellen), um den Migrationsprozess zu starten.



4. Sobald Sie auf die Schaltfläche **Create Volume** (Volume erstellen) geklickt haben, werden Sie darüber informiert, dass das Array erstellt wurde. Klicken Sie auf die Schaltfläche **OK**. Die Migration läuft nun im Hintergrund weiter. Der Computer kann während der Migration normal weiterverwendet werden.



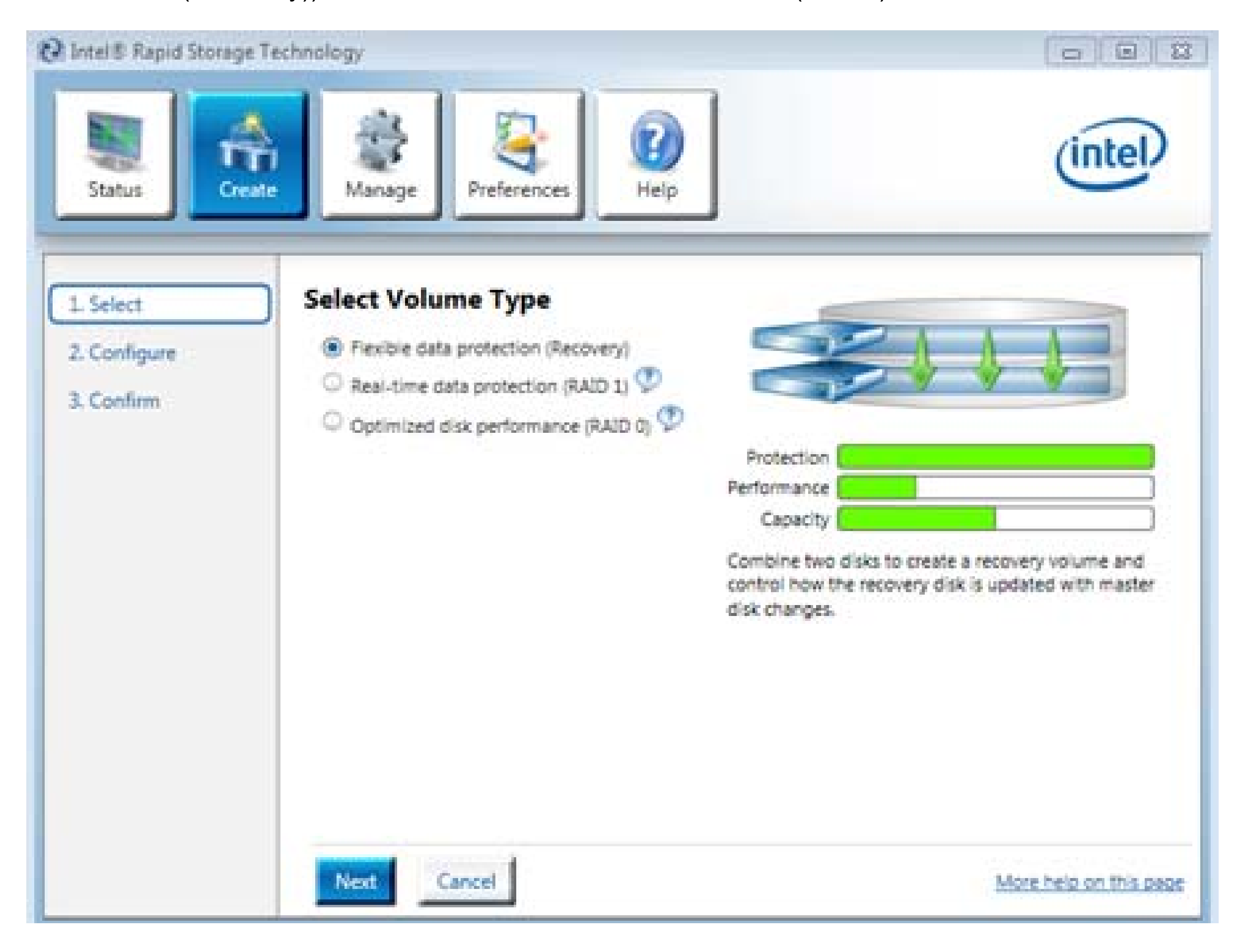
5. Wenn eine Meldung Sie darüber informiert, dass die Array-Migration abgeschlossen ist, schließen Sie alle geöffneten Programme, und starten Sie den Computer neu.

6. Beim Neustart des Computers erkennt das Betriebssystem das neu erstellte Array und fordert Sie zu einem zweiten Neustart auf. Starten Sie den Computer bei dieser Aufforderung neu. Nach diesem Neustart ist die RAID-Migration abgeschlossen.

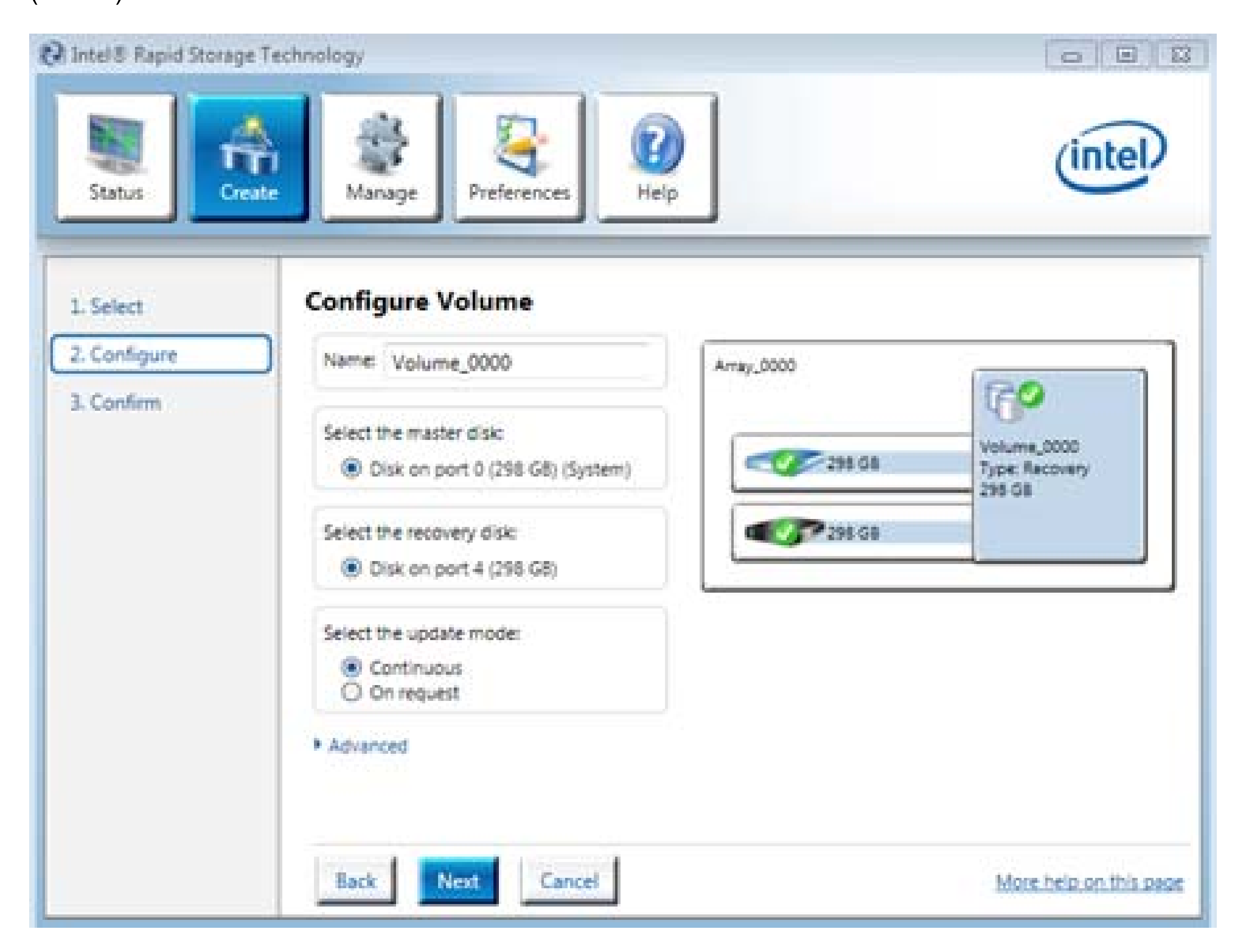
Migration nach Recovery

Recovery bietet eine größere Kontrolle über die Art und Weise, wie die Daten vom primären Laufwerk auf das Wiederherstellungslaufwerk kopiert werden. Wenn die sekundäre Festplatte im Schacht für SATA-Wechsellaufwerke der HP Advanced Docking Station installiert oder am eSATA-Anschluss (bestimmte Modelle) des Computers angeschlossen ist, ist Recovery die einzige verfügbare RAID-Option.

1. Klicken Sie auf **Create** (Erstellen), auf **Flexible data protection (Recovery)** (Flexibler Datenschutz (Recovery)), und klicken Sie anschließend auf **Next** (Weiter).



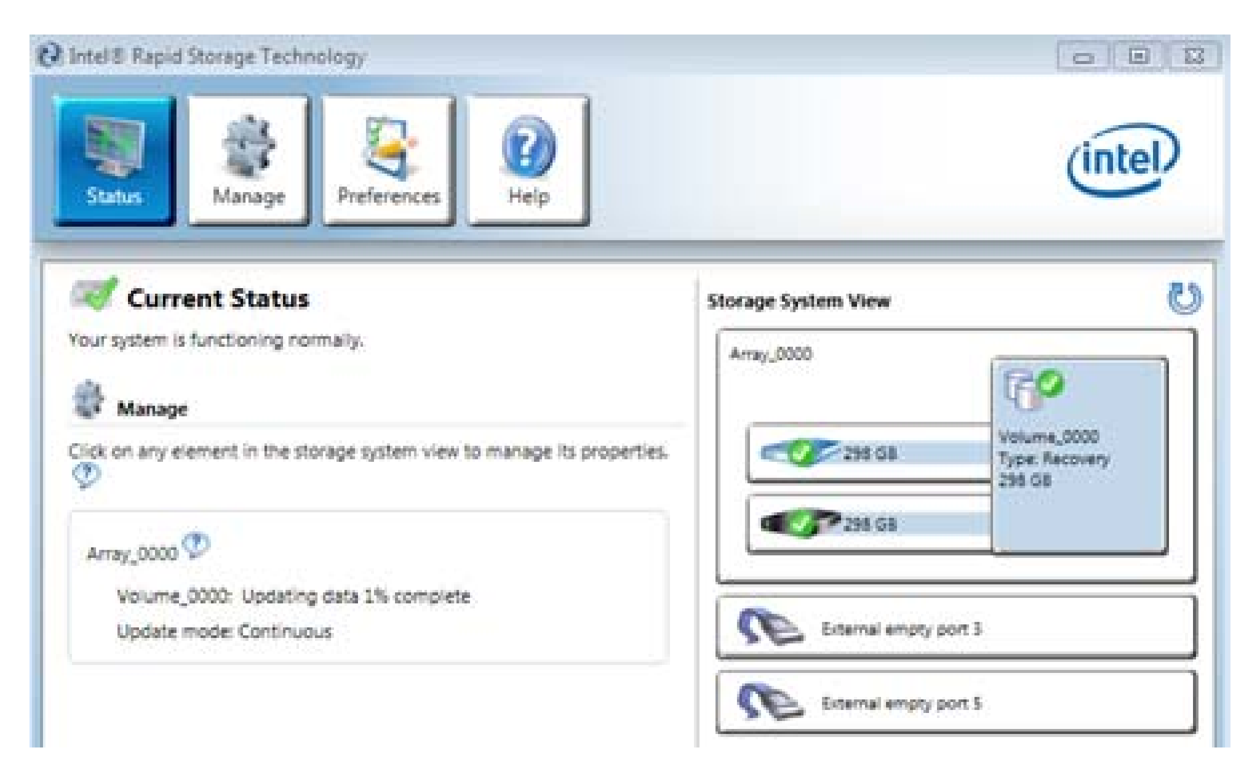
2. Erstellen Sie einen Volume-Namen (oder verwenden Sie den vorgeschlagenen Namen). Die beiden Festplatten für das Recovery-Array sind bereits ausgewählt. Klicken Sie auf **Next** (Weiter).



3. Klicken Sie auf **Create Volume** (Volume erstellen), um den Migrationsprozess zu starten.



4. Sobald Sie auf die Schaltfläche **Create Volume** (Volume erstellen) geklickt haben, werden Sie darüber informiert, dass das Array erstellt wurde. Klicken Sie auf die Schaltfläche **OK**. Die Migration läuft nun im Hintergrund weiter. Der Computer kann während der Migration normal weiterverwendet werden.

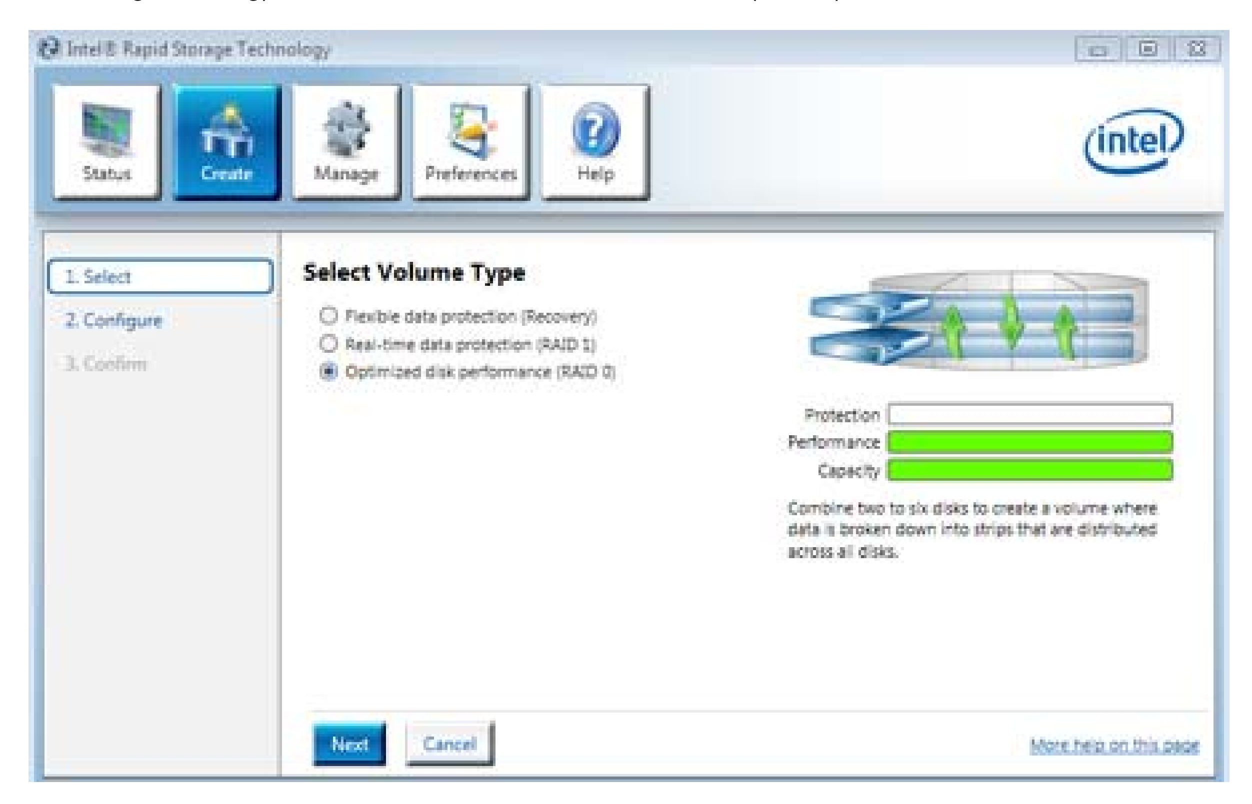


5. Wenn eine Meldung Sie darüber informiert, dass die Array-Migration abgeschlossen ist, schließen Sie alle geöffneten Programme, und starten Sie den Computer neu. Beim Neustart des Computers erkennt das Betriebssystem das neu erstellte Array und fordert Sie zu einem zweiten Neustart auf. Starten Sie den Computer bei dieser Aufforderung neu. Nach diesem Neustart ist die RAID-Migration abgeschlossen.

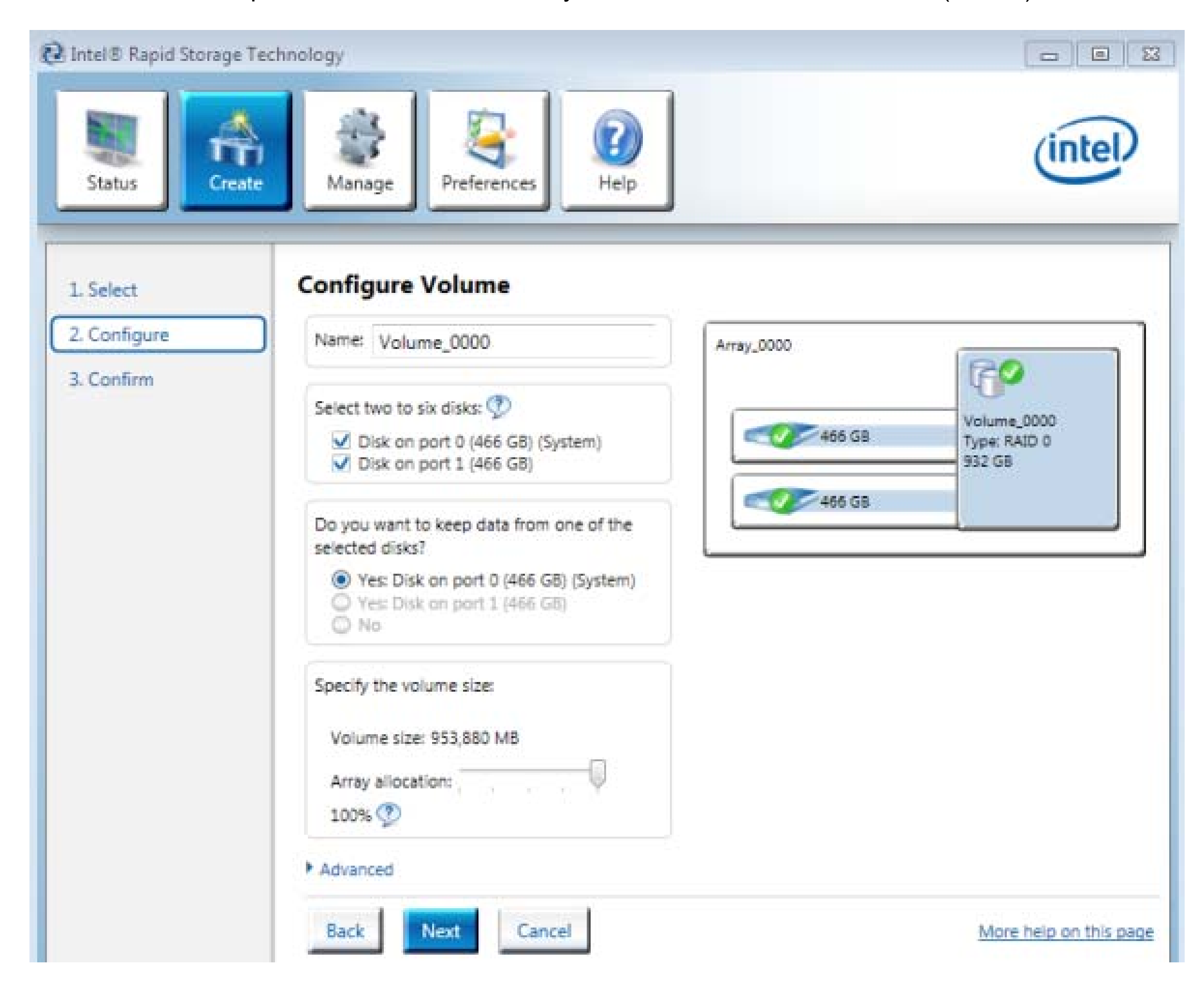
Migration auf RAID 0

HINWEIS: Wenn Sie ein von HP bereitgestelltes Image verwenden, müssen Sie für eine Migration nach RAID 0 einige zusätzliche Schritte durchführen, zum Beispiel Daten auf eine zusätzliche, externe USB-Festplatte kopieren. Lesen Sie zunächst die gesamte Anleitung für die RAID 0-Migration.

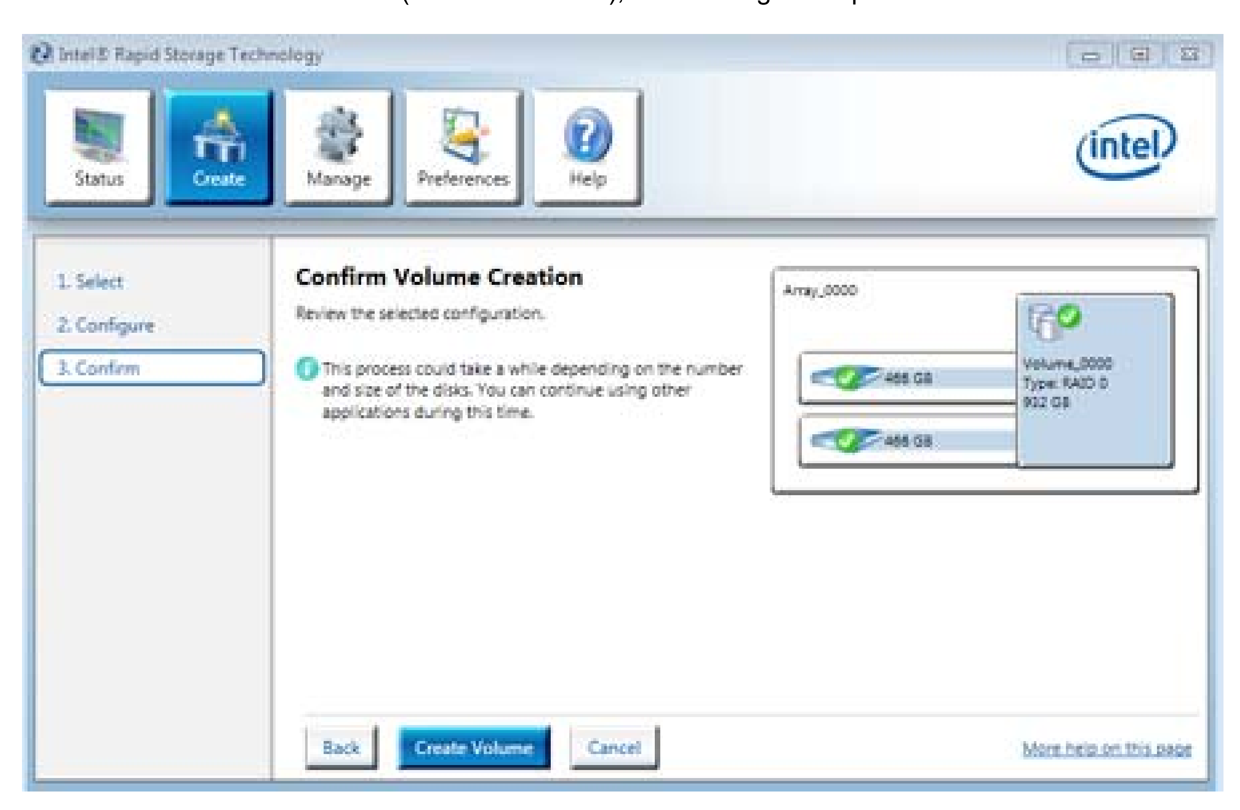
1. Klicken Sie auf **Create** (Erstellen), auf **Optimized disk performance** (Optimale Datenträgerleistung), und klicken Sie anschließend auf **Next** (Weiter).



2. Erstellen Sie einen Volume-Namen (oder verwenden Sie den vorgeschlagenen Namen), wählen Sie die beiden Festplatten für das RAID-0-Array, und klicken Sie dann auf **Next** (Weiter).

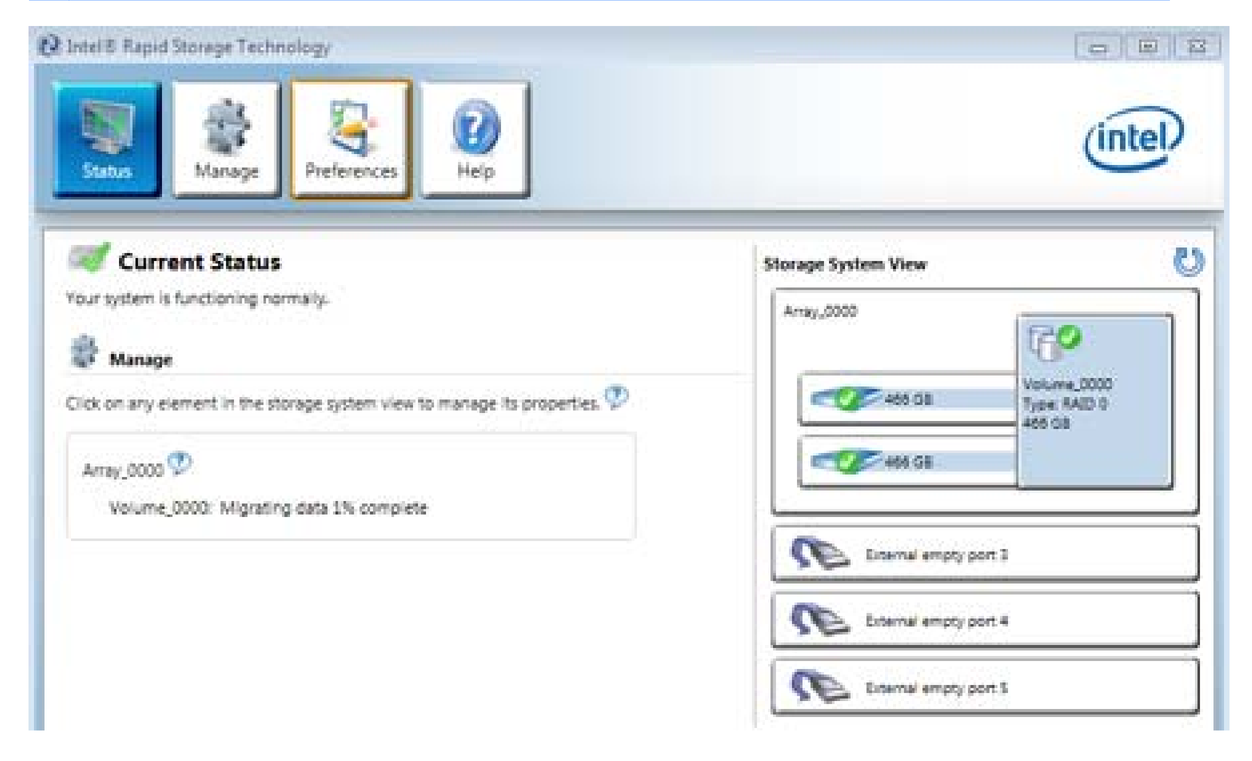


3. Klicken Sie auf **Create Volume** (Volume erstellen), um den Migrationsprozess zu starten.



4. Eine Meldung informiert Sie darüber, dass das Array erstellt wurde. Klicken Sie auf die Schaltfläche **OK**.

HINWEIS: Die Migration läuft nun im Hintergrund weiter. Der Computer kann während der Migration normal weiterverwendet werden.



5. Wenn eine Meldung Sie darüber informiert, dass die Array-Migration abgeschlossen ist, schließen Sie alle geöffneten Programme, und starten Sie den Computer neu. Beim Neustart des Computers erkennt das Betriebssystem das neu erstellte Array und fordert Sie zu einem zweiten Neustart auf.

6. Nachdem Sie den Computer ein zweites Mal neu gestartet haben, ist die RAID-Migration abgeschlossen.

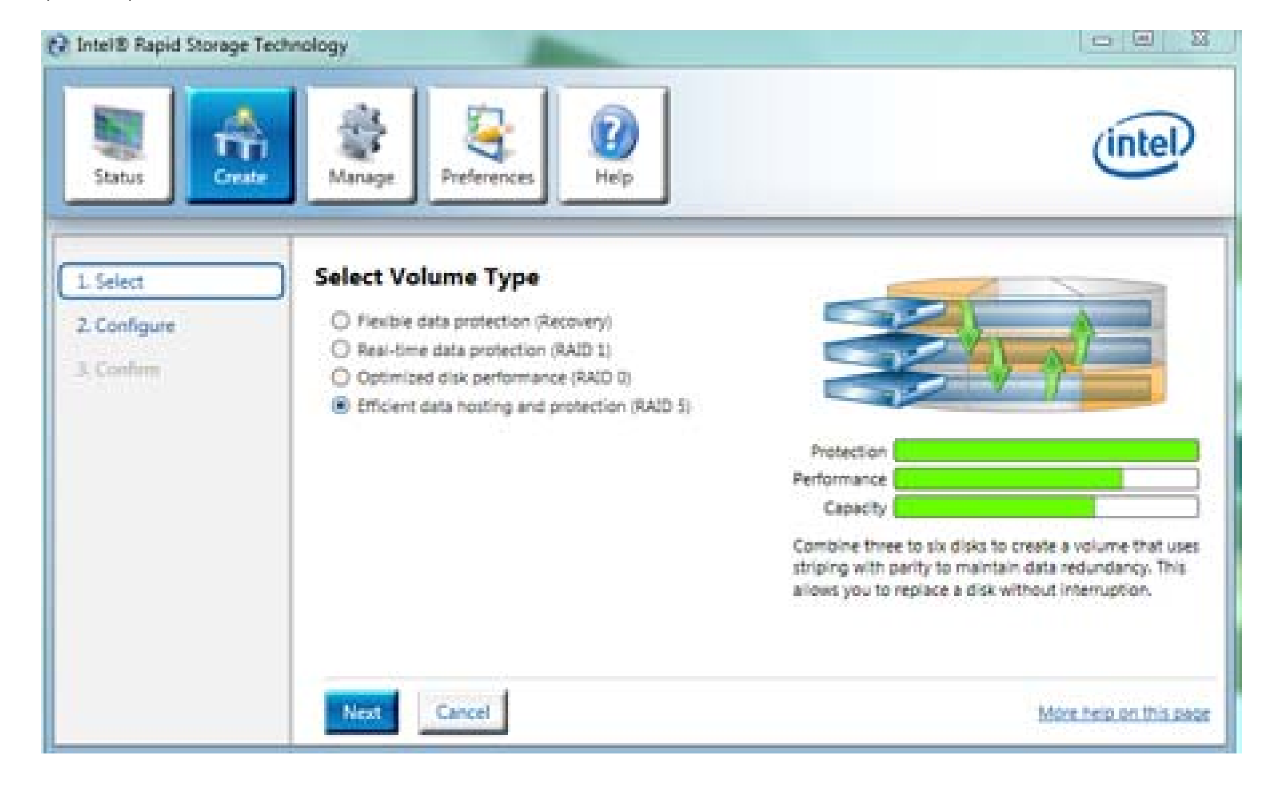
HINWEIS: In der Konsole wird zwar die Gesamtkapazität des RAID 0-Volume angezeigt, die zusätzliche Kapazität durch das Hinzufügen der sekundären Festplatte erscheint dem System gegenüber jedoch als nicht zugeordneter Speicherplatz. Nach dem Systemneustart müssen Sie den bisher nicht zugeordneten Speicherplatz zuordnen. Unter Windows XP besteht die einzige Option hierzu darin, ein separates Volume zu erstellen und zu formatieren. Unter Windows Vista und Windows 7 stehen Ihnen Funktionen zur Verfügung, mit denen Sie ein einziges RAID 0-Volume erstellen können. Weitere Anleitungen finden Sie unter „Zuordnen von nicht zugeordnetem Festplattenplatz für ein HP Image“ auf Seite 32.

Migration nach RAID 5 (bestimmte Modelle)

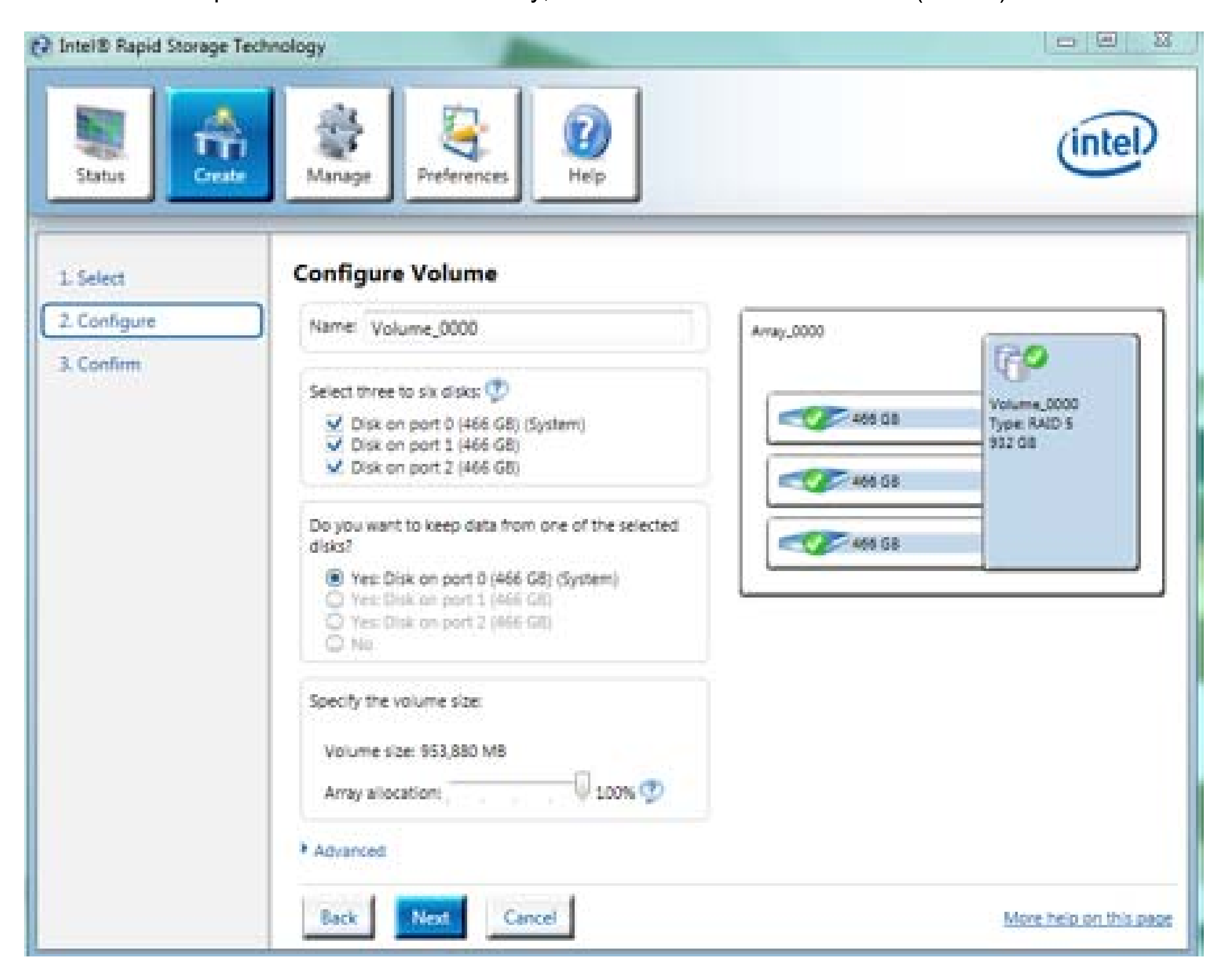
HINWEIS: Wenn Sie ein von HP bereitgestelltes Image verwenden, müssen Sie für eine Migration nach RAID 5 einige zusätzliche Schritte durchführen, zum Beispiel Daten auf eine zusätzliche, externe USB-Festplatte kopieren. Lesen Sie zunächst die gesamte Anleitung für die RAID 5-Migration.

HINWEIS: Für RAID 5 sind drei Festplatten im Computer erforderlich: die primäre Festplatte, die sekundäre Festplatte und die Festplatte im Erweiterungsschacht.

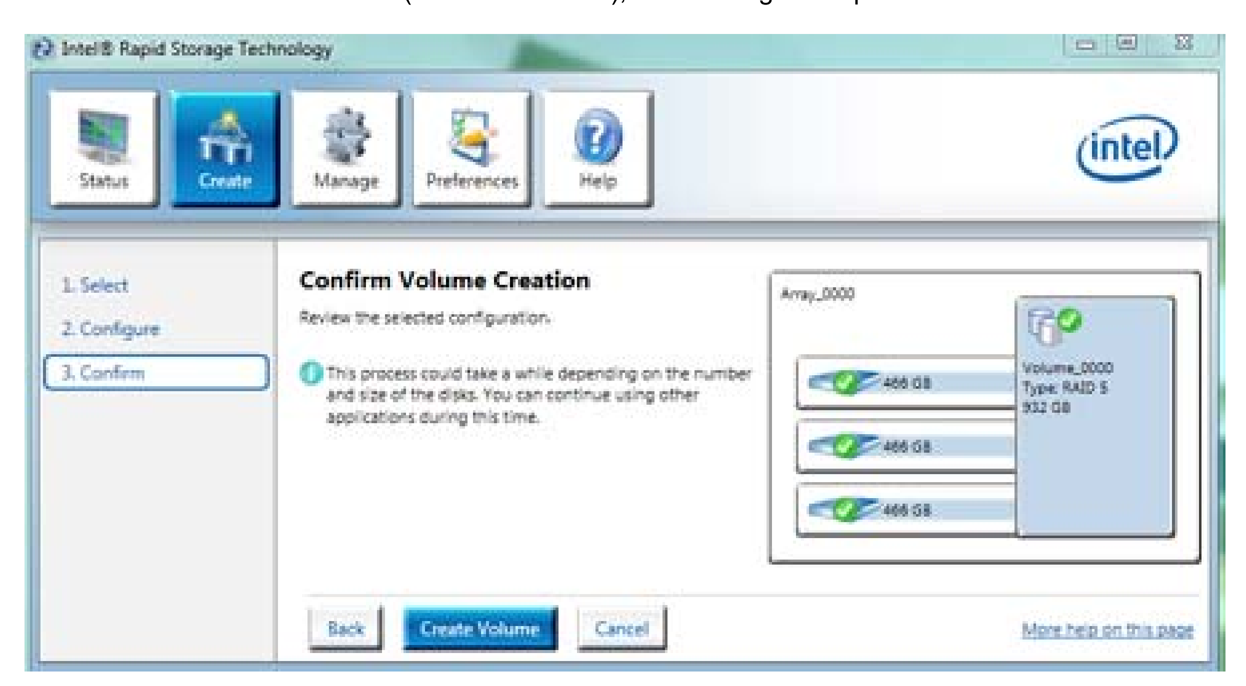
1. Klicken Sie auf **Create** (Erstellen), auf **Efficient data hosting and protection (RAID 5)** (Effizienter Datendurchsatz und Datenschutz (RAID 5)), und klicken Sie anschließend auf **Next** (Weiter).



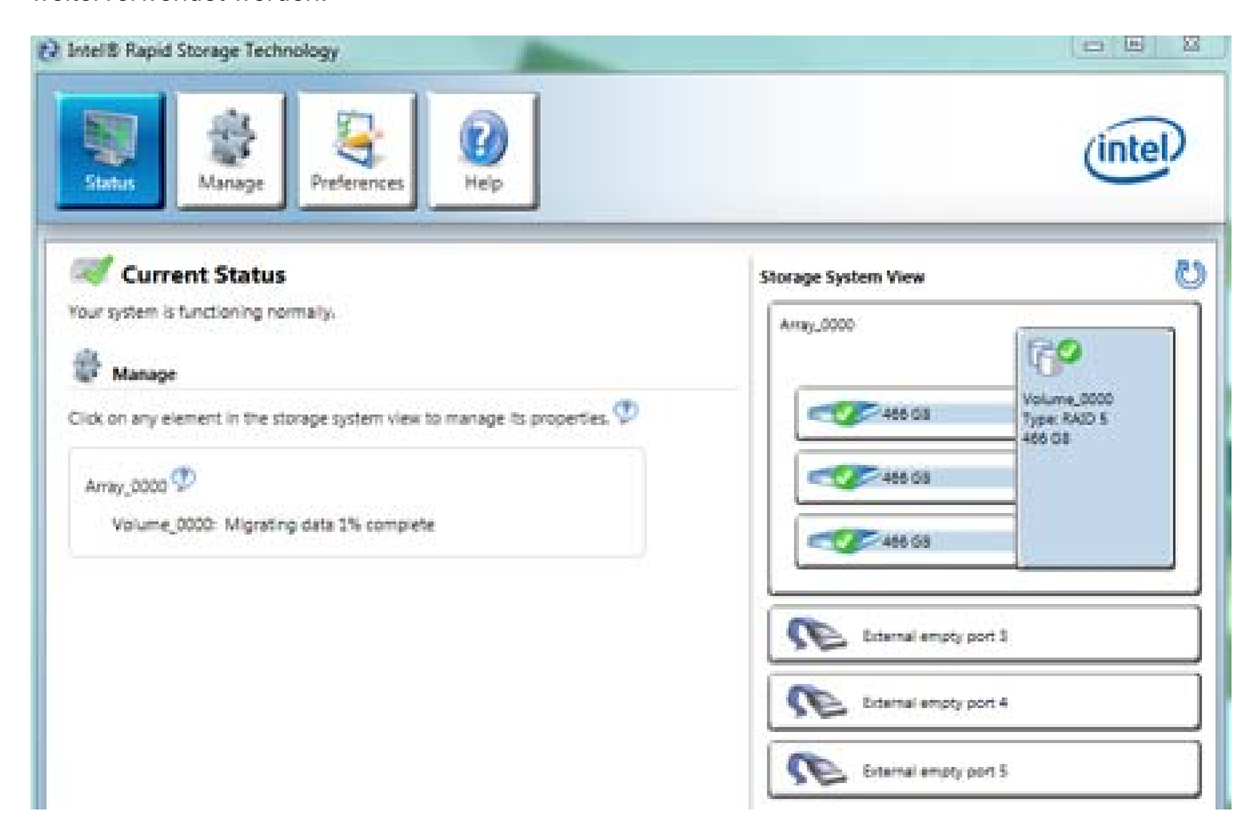
2. Erstellen Sie einen Volume-Namen (oder verwenden Sie den vorgeschlagenen Namen), wählen Sie die drei Festplatten für das RAID 5-Array, und klicken Sie dann auf **Next** (Weiter).



3. Klicken Sie auf **Create Volume** (Volume erstellen), um den Migrationsprozess zu starten.



4. Sobald Sie auf die Schaltfläche **Create Volume** (Volume erstellen) geklickt haben, werden Sie darüber informiert, dass das Array erstellt wurde. Klicken Sie auf die Schaltfläche **OK**. Die Migration läuft nun im Hintergrund weiter. Der Computer kann während der Migration normal weiterverwendet werden.



5. Wenn eine Meldung Sie darüber informiert, dass die Array-Migration abgeschlossen ist, schließen Sie alle geöffneten Programme, und starten Sie den Computer neu. Beim Neustart

des Computers erkennt das Betriebssystem das neu erstellte Array und fordert Sie zu einem zweiten Neustart auf.

6. Nachdem Sie den Computer ein zweites Mal neu gestartet haben, ist die RAID-Migration abgeschlossen.

HINWEIS: In der Konsole wird zwar die Gesamtkapazität des RAID 5-Volume angezeigt, die zusätzliche Kapazität durch das Hinzufügen der drei Laufwerke erscheint dem System gegenüber jedoch als nicht zugeordneter Speicherplatz. Nach dem Systemneustart müssen Sie den bisher nicht zugeordneten Speicherplatz zuordnen. Unter Windows XP besteht die einzige Option hierzu darin, ein separates Volume zu erstellen und zu formatieren. Unter Windows Vista und Windows 7 stehen Ihnen Funktionen zur Verfügung, mit denen Sie ein einziges RAID 5-Volume erstellen können. Weitere Anleitungen finden Sie unter „Zuordnen von nicht zugeordnetem Festplattenplatz für ein HP Image“ auf Seite 32.

Zuordnen von nicht zugeordnetem Festplattenplatz für ein HP Image

Wenn Sie eine zusammenhängende Partition C: für RAID 0 und RAID 5 wünschen, müssen Sie nach dem letzten Systemneustart den nicht zugeordneten Speicherplatz zuordnen. Sie können eine zusätzliche Partition erstellen oder die Partition (C:) erweitern. Um die Partition (C:) zu erweitern, müssen Sie wie im Folgenden beschrieben die Partition mit dem Extensible Firmware Interface (EFI) und die Recovery-Partition verschieben. Auf der EFI-Partition sind die Dateien für QuickLook, Systemdiagnose und BIOS-Flash-Wiederherstellung gespeichert. Die Recovery-Partition enthält Dateien für die Wiederherstellung des Auslieferungszustands des Computers.

HINWEIS: Wenn die Funktionalitäten der EFI- und Recovery-Partitionen nicht benötigt werden, können diese Partitionen gelöscht werden.

Unter Windows XP:

1. Klicken Sie nach dem Systemneustart auf **Start** und dann mit der rechten Maustaste auf **Arbeitsplatz**. Wählen Sie aus dem Kontextmenü die Option **Verwalten**.

2. Klicken Sie im linken Fensterbereich unter **Datenspeicher** auf **Datenträgerverwaltung**. Im Fenster für die Datenträgerverwaltung werden der nicht zugeordnete Speicherplatz und zwei Partitionen angezeigt: (C:) und HP_TOOLS.

3. Klicken Sie mit der rechten Maustaste auf die **Nicht zugeordnete** Speicherkapazität, und wählen Sie im Kontextmenü die Option **Neue Partition**. Der Assistent zum Erstellen neuer Partitionen wird geöffnet.

4. Klicken Sie auf **Weiter**.

5. Wählen Sie **Primäre Partition**, und klicken Sie dann auf **Weiter**.

   Die Größe der Partition wird automatisch auf den maximalen Wert gesetzt.

6. Klicken Sie auf **Weiter**.

7. Weisen Sie der Partition einen Laufwerkbuchstaben zu, und klicken Sie auf **Weiter**.

8. Wählen Sie als Format **NTFS**, benennen Sie das Volume, und klicken Sie dann auf **Weiter**.

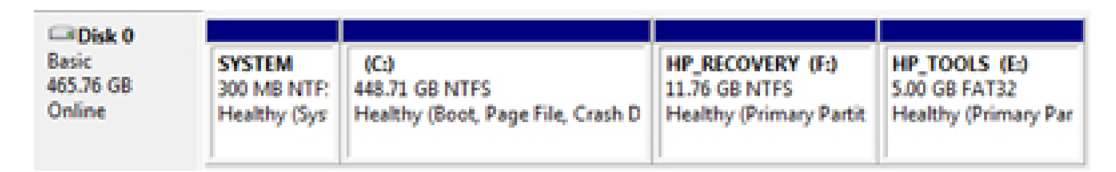
9. Kontrollieren Sie die vorgenommenen Einstellungen, und klicken Sie dann auf **Fertig stellen**.

Unter Windows Vista und Windows 7:

1. Klicken Sie auf **Start** und dann mit der rechten Maustaste auf **Computer**. Wählen Sie aus dem Kontextmenü die Option **Verwalten**. Das Fenster **Computerverwaltung** wird geöffnet.

2. Klicken Sie im linken Fensterbereich unter **Datenspeicher** auf **Datenträgerverwaltung**. Das Fenster für die Datenträgerverwaltung wird geöffnet und zeigt die vorhandenen Partitionen sowie nicht zugeordneten Speicherplatz an: (C:), HP_TOOLS und HP_RECOVERY. Notieren Sie sich die Größe der Partition HP_RECOVERY (z. B. 11,76 GB), und bewahren Sie diese Angaben für den nächsten Schritt auf.

HINWEIS: Je nach Konfiguration Ihres Systems werden unter Datenträgerverwaltung möglicherweise andere Laufwerksbuchstaben angezeigt.



3. Schließen Sie an einen USB-Anschluss des Computers ein externes USB-Laufwerk mit mindestens 40 GB freier Kapazität an.

4. Öffnen Sie Windows Explorer, und wählen Sie das primäre Laufwerk **(C:)** aus.

5. Wählen Sie **Organisieren > Ordner- und Suchoptionen**.

6. Klicken Sie auf die Registerkarte **Ansicht**.

7. Aktivieren Sie unter **Versteckte Dateien und Ordner** die Optionsschaltfläche neben **Alle Dateien und Ordner anzeigen**.

8. Deaktivieren Sie das Kontrollkästchen **Geschützte Systemdateien ausblenden**, und klicken Sie dann auf **OK**.

9. Wählen Sie im linken Fensterbereich die Partition **HP_RECOVERY**, und kopieren Sie dann deren Inhalt (\boot, \Recovery, \system.save, bootmgr und HP_WINRE) auf das externe USB-Laufwerk. Wenn die Meldung „Zugriff auf den Zielordner wurde verweigert“ angezeigt wird, klicken Sie auf **Fortsetzen**, um die Datei zu kopieren. Wenn das Fenster **Benutzerkontensteuerung** geöffnet wird, klicken Sie auf **Fortsetzen**.

10. Wählen Sie im linken Fensterbereich die Partition **HP_TOOLS**, und kopieren Sie ihren Inhalt (Hewlett-Packard, HP_Tools) auf das USB-Laufwerk.

11. Wechseln Sie zurück zum Fenster der Datenträgerverwaltung, und wählen Sie die Partition **HP_RECOVERY**. Klicken Sie dann in der Menüleiste auf das Symbol **Löschen**. Wiederholen Sie diesen Vorgang für die Partition HP_TOOLS. Der erforderliche Speicherplatz für die Wiederherstellung von HP_RECOVERY und HP_TOOLS muss berechnet werden.

So berechnen Sie den für die Wiederherstellung von HP_RECOVERY und HP_TOOLS erforderlichen Speicherplatz und rechnen die Größe der Partition HP_RECOVERY von Gigabyte (GB) in Megabyte (MB) um:

a. Multiplizieren Sie die Größe der Partition HP_RECOVERY (siehe Schritt 2 oben) mit 1024, und runden Sie das Ergebnis auf. Multiplizieren Sie beispielsweise 11,76 GB mit 1024, und runden Sie das Ergebnis (12042,24 MB) auf 12043 MB auf.

b. Multiplizieren Sie die Größe von HP_TOOLS mit 1024, und runden Sie anschließend das Ergebnis auf. Wenn die Größe der Partition HP_TOOLS beispielsweise 5 GB beträgt, lautet das Ergebnis 5120 MB.

c. Berechnen Sie den Speicherplatz der Metadaten (z. B. 6 MB) am Ende der Festplatte, und addieren Sie diese drei Werte (z. B. 12043 MB + 5120 MB + 6 MB = 17169 MB). Das Ergebnis ist der Speicherplatz, der für die Wiederherstellung der HP Verzeichnisse erforderlich ist.

12. Klicken Sie mit der rechten Maustaste auf das Laufwerk **(C:)**, und wählen Sie im Dropdown-Menü die Option **Volume erweitern**. Der Assistent zum Erweitern von Volumes wird geöffnet.

13. Klicken Sie auf **Weiter**.

14. Die Menge an nicht zugeordnetem Speicher (in MB), die für die Erweiterung von Laufwerk (C:) zur Verfügung steht, wird neben der Angabe **Speicherplatz in MB** (z. B. 494098 MB) angezeigt. Subtrahieren Sie den Wert des für die Wiederherstellung der HP Verzeichnisse erforderlichen Speicherplatzes (wie oben berechnet) von der Menge des nicht zugeordneten Speicherplatzes (in MB), der für die Erweiterung von Laufwerk (C:) erforderlich ist. Beispiel: 494098 MB – 17169 MB = 476929 MB. Ersetzen Sie den **Speicherplatz in MB** durch den berechneten Wert (z. B. 476929 MB), oder drücken Sie die Nach-unten-Taste, bis der berechnete Wert angezeigt wird.

15. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Im Fenster für die Datenträgerverwaltung werden nun die neue Kapazität des RAID-Volume sowie der nicht zugeordnete Speicher angezeigt.

16. Erstellen Sie die Partition HP_RECOVERY folgendermaßen:

    a. Klicken Sie mit der rechten Maustaste auf die **Nicht zugeordnete** Speicherkapazität, und wählen Sie im Kontextmenü die Option **Neues einfaches Volume**. Der Assistent zum Erstellen neuer einfacher Volumes wird geöffnet.

    b. Klicken Sie auf **Weiter**.

    c. Geben Sie den aufgerundeten Wert aus Schritt 11a oben in das entsprechende Feld ein, und klicken Sie anschließend auf **Weiter**.

    d. Wählen Sie den Laufwerkbuchstaben **(E:)**, und klicken Sie dann auf **Weiter**.

    e. Wählen Sie **NTFS** als Dateisystem. Geben Sie als Volumebezeichnung den Namen HP_RECOVERY ein.

    f. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

17. Die folgenden Schritte sind erforderlich, um die Partition HP_TOOLS zu erstellen. Diese zusätzlichen Schritte sind erforderlich, da die Partition HP_TOOLS als primäre Partition erstellt werden muss. Wenn die Datenträgerverwaltung verwendet wird, wird die Partition als logisches Laufwerk erstellt.

Disk 0 Basic 298.10 GB Online	(C:) 278.09 GB NTFS Healthy (System, Boot, Page File, Active,	HP_TOOLS (E:) 5.00 GB FAT32 Healthy (Primary Partition)	HP_RECOVERY (D:) 15.00 GB NTFS Healthy (Primary Partition)

a. Öffnen Sie eine als Administrator ausgeführte Befehlszeile (**Start > Alle Programme > Zubehör**).

b. Klicken Sie mit der rechten Maustaste auf **Eingabeaufforderung**, wählen Sie die Option **Als Administrator ausführen**, und geben Sie anschließend die folgenden Befehle ein:

Diskpart

Select disk 0

Create part primary size=5120

Format fs=fat32 label="HP_TOOLS" quick

Assign

Exit

18. Starten Sie den Computer neu.

19. Kopieren Sie in Windows Explorer den Inhalt von HP_TOOLS und HP_RECOVERY vom USB-Laufwerk auf die entsprechenden Partitionen.

20. Damit alle Funktionen von HP Recovery (f11 während des POST) ordnungsgemäß ausgeführt werden, müssen die Bootkonfigurationsdaten (BCD) aktualisiert werden. Die folgenden Befehle müssen im Administratormodus ausgeführt werden. Es wird empfohlen, eine Batch-Datei (*.bat) mit diesen Befehlen zu erstellen und diese dann auszuführen, anstatt jeden Befehl von Hand einzugeben.

HINWEIS: Bei diesen Befehlen wird davon ausgegangen, dass die Partition HP_RECOVERY den Laufwerksbuchstaben (E:) hat. Ist dies nicht der Fall, ersetzen Sie E: durch den korrekten Laufwerksbuchstaben.

BCDEDIT.EXE -store E:\Boot\BCD -create {ramdiskoptions} -d "Ramdisk Options"

BCDEDIT.EXE -store E:\Boot\BCD -set {ramdiskoptions} ramdisksdidevice partition=E:

BCDEDIT.EXE -store E:\Boot\BCD -set {ramdiskoptions} ramdisksdipath \boot\boot.sdi

BCDEDIT.EXE -store E:\Boot\BCD -create {572bcd55-ffa7-11d9-aae0-0007e994107d} -d "HP Recovery Environment" -application OSLOADER

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} device ramdisk=[E:]\Recovery\WindowsRE\winre.wim,{ramdiskoptions}

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} path \windows\system32\boot\winload.exe

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} osdevice ramdisk=[E:]\Recovery\WindowsRE\winre.wim,{ramdiskoptions}

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} systemroot \windows

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} winpe yes

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} detecthal yes

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} nx optin

BCDEDIT.EXE -store E:\Boot\BCD -set {572bcd55-ffa7-11d9-aae0-0007e994107d} custom: 46000010 yes

BCDEDIT.EXE -store E:\Boot\BCD -create {bootmgr} /d "Windows Boot Manager"

BCDEDIT.EXE -store E:\Boot\BCD -set {bootmgr} device boot

BCDEDIT.EXE -store E:\Boot\BCD -set {bootmgr} displayorder {default}

BCDEDIT.EXE -store E:\Boot\BCD -set {bootmgr} default {572bcd55-ffa7-11d9-aae0-0007e994107d}

21. Nachdem Sie die Batch-Datei erstellt haben, klicken Sie in Windows Explorer mit der rechten Maustaste darauf, und wählen Sie die Option **Als Administrator ausführen**, um die Batch-Datei auszuführen.

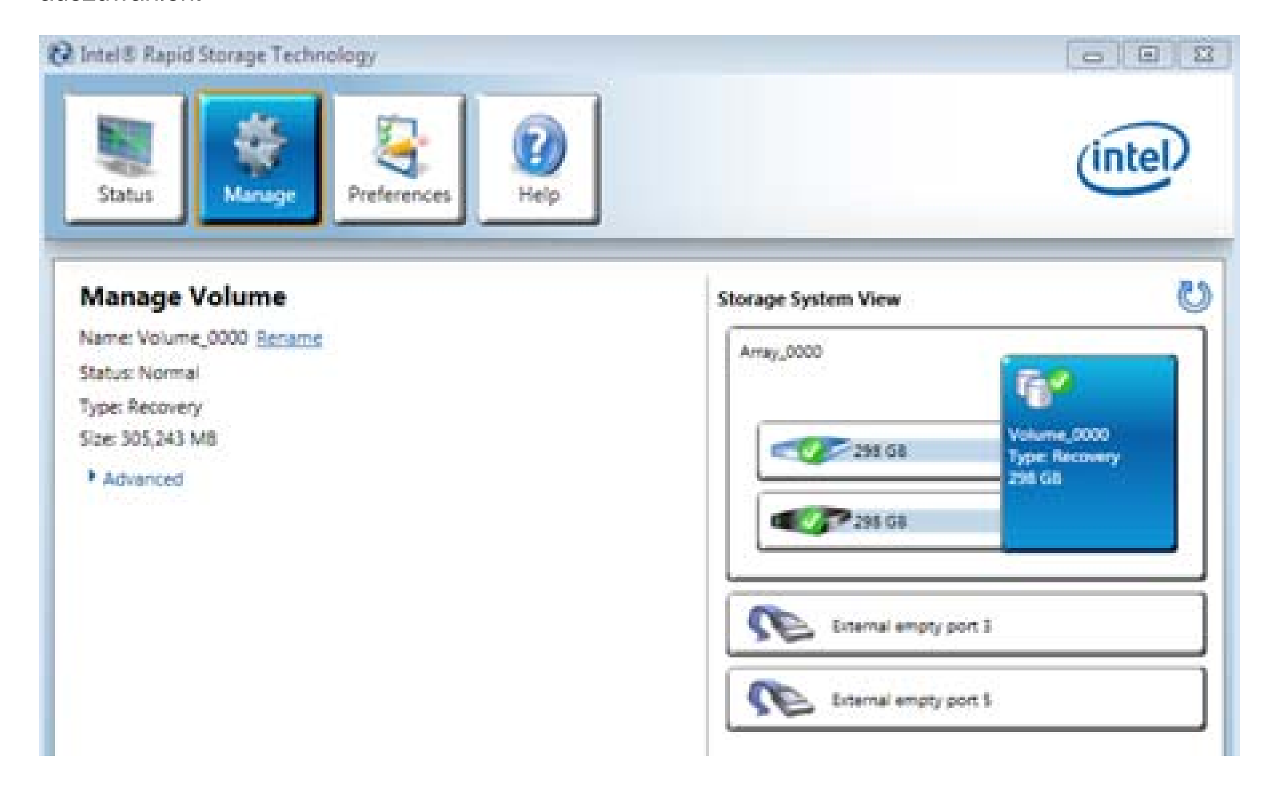
22. Starten Sie den Computer neu.

Verwenden der Recovery-Merkmale von Intel Rapid Storage Technology Console

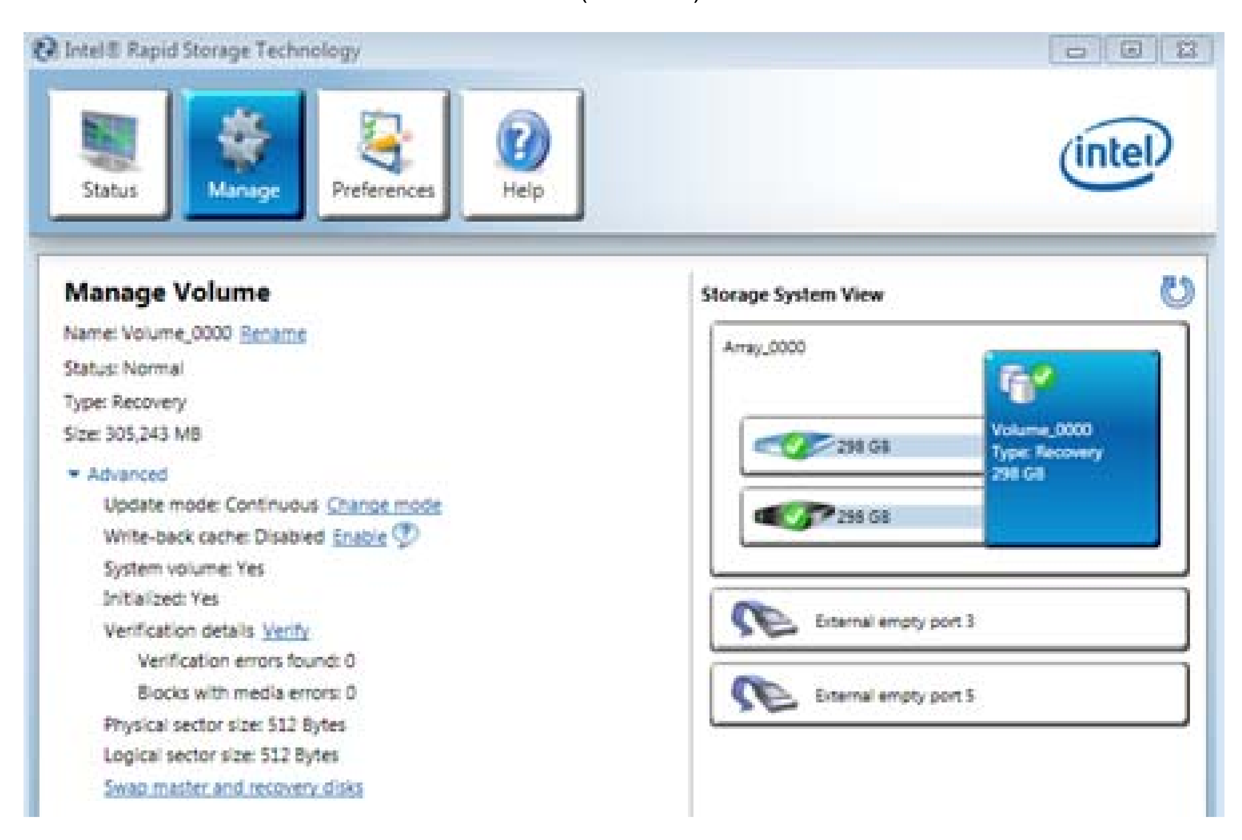
Ändern der Aktualisierungsweise für das Volume

Wenn Sie Recovery verwenden, können Sie auswählen, wie oft die Wiederherstellungsfestplatte aktualisiert werden soll: „Continuous“ (ständig) oder „On request“ (auf Anforderung). Die ständige Aktualisierung ist die Standardeinstellung (siehe „Vorgehensweisen zum Aktualisieren des Spiegellaufwerks“ auf Seite 12). So stellen Sie die Aktualisierung auf Anforderung ein:

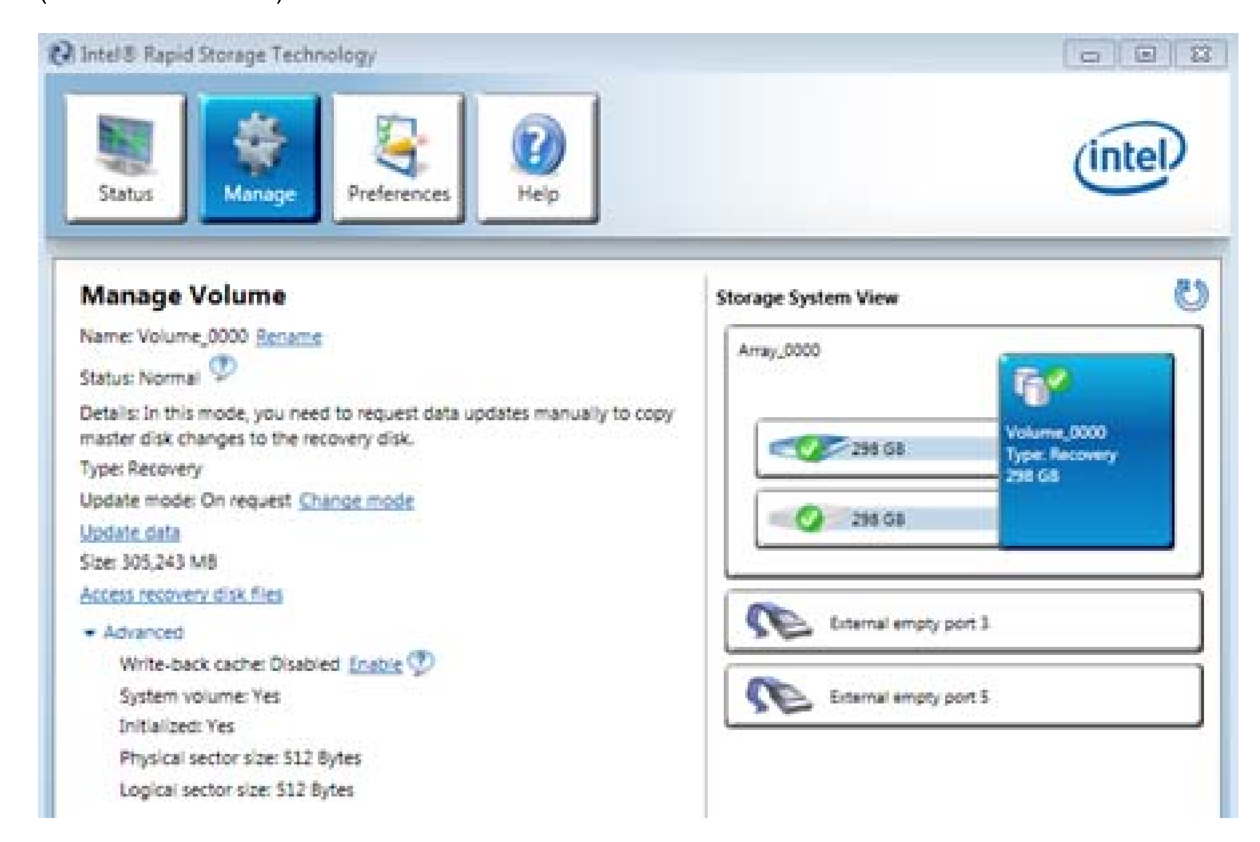
1. Klicken Sie auf **Manage** (Verwalten), und klicken Sie auf das Recovery-Volume, um es auszuwählen.



2. Klicken Sie auf der linken Seite auf **Advanced** (Erweitert).



3. Im Update-Modus wird die aktuelle Einstellung angezeigt. Um die aktuelle Einstellung zu ändern, klicken Sie auf den Link **Change Mode** (Modus ändern). Klicken Sie anschließend auf **Yes** (Ja). Wenn Sie die Aktualisierung auf Anforderung ausgewählt haben, können Sie das Volume für die Wiederherstellung manuell aktualisieren, indem Sie auf den Link **Update Data** (Daten aktualisieren) klicken.



4. Sie können jederzeit wieder die ständige Aktualisierung aktivieren, indem Sie auf den Link **Change Mode** (Modus ändern) und anschließend auf **Yes** (Ja) klicken.

6 Zurücksetzen von RAID-Laufwerken auf Nicht-RAID

Sie können aus einem RAID 1- oder Recovery-Volume wieder zwei Nicht-RAID-Laufwerke erstellen. Hierzu müssen Sie nach folgender Anleitung auf das Intel Options-ROM zugreifen und beide Laufwerke auf den Status Nicht-RAID zurücksetzen. Sie müssen beide Laufwerke auch dann zurücksetzen, wenn Sie das RAID-Wiederherstellungslaufwerk vom Erweiterungsschacht des Computers in den Schacht der Dockingstation umsetzen möchten.

HINWEIS: Ein RAID 0-Volume oder ein RAID 5-Volume kann nicht nach einem RAID 1-Volume oder nach einer primären Nicht-RAID-Festplatte migriert werden, da die Größe des RAID 0-Volume bzw. des RAID 5-Volume möglicherweise größer ist als die Kapazität der primären Festplatte. Wenn Sie die primäre Festplatte in einem RAID 0-Volume bzw. einem RAID 5-Volume in den Nicht-RAID-Status zurückversetzen möchten, müssen Sie zuerst alle Daten auf einem externen Laufwerk mit ausreichender Kapazität sichern. Dann setzen Sie gemäß der folgenden Anleitung die RAID 0-Laufwerke bzw. der RAID 5-Laufwerke auf Nicht-RAID zurück. Nach Beendigung des Vorgangs müssen Sie auf dem primären Laufwerk das Betriebssystem neu installieren.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Wenn das Options-ROM-Fenster angezeigt wird, drücken Sie strg+I, um das Konfigurationsprogramm zu öffnen.

```
Intel(R) Rapid Storage Technology - Option ROM - 10.1.1.1003
Copyright(C) 2003-10 Intel Corporation. All Rights Reserved.

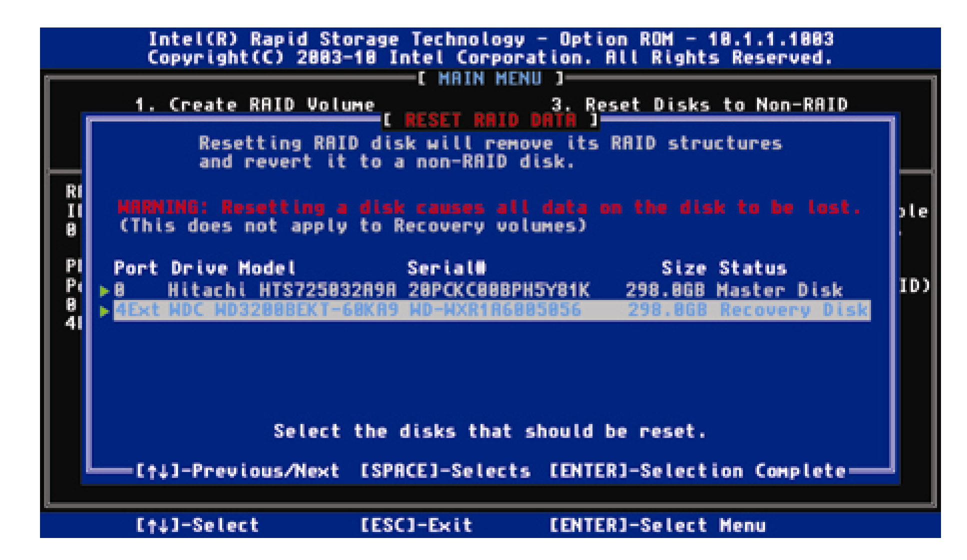
  RAID Volumes:
  ID   Name             Level             Strip      Size Status     Bootable
  0    Volume_000       Recovery(cont.)   N/A      298.1GB Updated      Yes

  Physical Devices:
  Port Device Model     Serial #                     Size Type/Status(Vol ID)
  0    Hitachi HTS72503 20PCKC00BPH5Y01K           298.0GB Master Disk(0)
  4Ext WDC WD3200BEKT-6 WD-WXR1A6005056            298.0GB Master Disk(0)

Press <CTRL-I> to enter Configuration Utility..
```

2. Wählen Sie im Hauptmenü mithilfe der Pfeiltasten den Punkt **3. Reset Disks to Non-RAID** (3. Laufwerke auf Nicht-RAID zurücksetzen) aus, und drücken Sie dann die Eingabetaste. Das Fenster **Reset RAID Data** (Zurücksetzen der RAID-Daten) wird angezeigt.

3. Wählen Sie mithilfe der Leertaste das erste Laufwerk aus, drücken Sie dann die Nach-unten-Taste und dann die Leertaste, um das zweite Laufwerk auszuwählen.



4. Drücken Sie die Eingabetaste und dann die y-Taste, um die Auswahl zu bestätigen.

5. Wählen Sie mithilfe der Nach-unten-Taste den Menüpunkt **Exit** (Beenden), bestätigen Sie mit der Eingabetaste, und starten Sie dann mit y das System neu.

7 Häufige Fragen

Kann auf einem Computer mehr als ein RAID-Volume erstellt werden?

Nein, auf einem Computer kann es nur ein RAID-Volume geben.

Ist in einem einzigen RAID-Volume sowohl RAID 0 als auch RAID 1 möglich?

Nein.

Kann der Computer abgedockt werden, wenn sich die Wiederherstellungsfestplatte im Schacht für SATA-Wechsellaufwerke der Dockingstation befindet?

Ja. Wenn die Aktualisierungsart „Continuous“ (ständig) ausgewählt ist, werden die Daten automatisch auf das Wiederherstellungslaufwerk in der Dockingstation kopiert, sobald der Computer wieder angedockt wird. Ist „On request“ (Aktualisierung auf Anfrage) ausgewählt, müssen Sie nach dem Andocken die Daten auf der Wiederherstellungsfestplatte nach der gewohnten Methode aktualisieren.

Wie viele Festplatten können maximal während des Starts an das System angeschlossen sein, wenn sich der Speicher-Controller im RAID-Modus (f10 Computer Setup) befindet?

Diese Beschränkung gilt nicht, wenn sich der Speicher-Controller im AHCI-Modus befindet. Sobald sich der Speicher-Controller wieder im RAID-Modus befindet, können während der Systemstarts nur 3 Festplatten an das System angeschlossen sein. Nach dem Systemstart können weitere Festplatten angeschlossen werden. Dies gilt nicht für angeschlossene USB-Festplatten.

Index

